BitDefender 8 SpamDeny

Manuel d'utilisation



Index

1

Accord de licence

Licence du logiciel

Le package BitDefender est protégé par la loi du copyright et par les traités internationaux concernant le copyright aussi bien que par d'autres lois et traités concernant la propriété intellectuelle. La loi du copyright, aussi bien que d'autres lois de la propriété intellectuelle, protège dans beaucoup de pays les droits des propriétaires de logiciel, en leur accordant quelques droits exclusifs, comprenant le droit de reproduire et de copier le logiciel. La reproduction du logiciel sans la permission du propriétaire représente une "infraction de copyright" et la loi impose dans ce cas des pénalités et des punitions.

Le logiciel est considéré comme reproduit quand:

- Il est chargé dans la mémoire de votre ordinateur par l'intermédiaire du lecteur de disquettes, du disque dur, du CD-ROM, ou d'autres medias;
- Il est copié sur un autre support, tel que la disquette ou le disque dur;
- Il est exécuté sur l'ordinateur depuis un serveur de réseau où le logiciel est résident ou déposé.

A peu près tout logiciel commercial est directement ou indirectement autorisé par le détenteur de copyright---le producteur du logiciel---pour usage final, par l'intermédiaire d'un contrat de licence. Des logiciels différents peuvent avoir différents types de contrats de licenciement.

BitDefender est une marque déposée de SOFTWIN. Microsoft, Windows, Excel, Word et les logos de Windows, Windows NT et Windows 2000 sont des marques déposées de Microsoft Corporation. Toutes autres marques déposées sont la propriété de leurs propriétaires respectifs.

Accord de licence

SI VOUS N'ACCEPTEZ PAS CES TERMES ET CONDITIONS, N'INSTALLEZ PAS CE LOGICIEL.
EN CLIQUANT SUR " OUI " OU EN INSTALLANT ET UTILISANT CE LOGICIEL, VOUS INDIQUEZ AVOIR COMPRIS ET ACCEPTÉ LES TERMES DE CET ACCORD.

Cet accord de licence est un accord légal entre vous (entité individuelle ou utilisateur final) et SOFTWIN pour l'usage du produit de SOFTWIN identifié au-dessus, qui comprend le logiciel et qui peut comprendre les éléments média, les matériels imprimés et la documentation " en ligne " ou électronique (" BitDefender "), le tout étant protégé par la loi française et par les lois et les traités internationaux. En installant, copiant, ou utilisant de toute autre manière le logiciel BitDefender, vous acceptez les termes de cet accord. Si vous n'agréez pas les termes de cet accord, n'installez pas et n'utilisez pas BitDefender.

BitDefender est protégé par les lois du copyright et par les traités internationaux concernant le copyright, ainsi que par les autres lois et traités concernant la propriété intellectuelle. BitDefender est licencié et non pas vendu.

Droits de licence Ce logiciel restant la propriété de SOFTWIN, vous disposez néanmoins de certains droits d'utilisation une fois l'accord de licence accepté. Vos droits et obligations relatifs à l'utilisation de ce logiciel sont les suivants:

LOGICIEL. Vous pouvez installer et utiliser une seule copie de BitDefender ou de toute version antérieure sur le même système d'exploitation, sur un seul poste de travail. L'utilisateur principal de l'ordinateur, sur lequel BitDefender est installé, peut faire une copie additionnelle (seconde) pour son usage exclusif ou pour l'usage sur un ordinateur portable.

USAGE EN RÉSEAU. Vous pouvez emmagasiner ou installer une copie de BitDefender sur un dispositif de stockage, comme le serveur de réseau, employé seulement pour installer ou exécuter sur les autres ordinateurs d'un réseau interne ; néanmoins, vous devez acheter et dédier une licence séparée pour chaque terminal d'ordinateur sur lequel BitDefender est installé ou exécuté depuis le dispositif de stockage. Une licence de BitDefender ne peut pas être partagée ou utilisée de manière concurrentielle sur des postes ou terminaux d'ordinateurs multiples. Vous devrez acheter un pack de licences si vous en envisagez l'usage sur différents ordinateurs.

PACK DE LICENCES. Si vous achetez un Pack de Licences et que vous ayez acquis cet Accord de licence pour plusieurs licences de BitDefender, vous pouvez réaliser le nombre de copies du logiciel spécifié au-dessus comme "Copies licenciées". Vous avez aussi le droit de réaliser un nombre correspondant de copies pour l'usage sur des ordinateurs portables, comme spécifié ci-dessus dans la section "LOGICIEL".

TERMES DE LA LICENCE. La licence accordée ci-dessus commencera au moment où vous installez, copiez ou utilisez de toute autre manière BitDefender pour la première fois et continuera seulement pour l'ordinateur sur lequel le logiciel a été premièrement installé.

MISES À JOUR. Si BitDefender constitue une mise à jour, vous devez être correctement licencié pour utiliser le produit identifié par SOFTWIN comme étant éligible pour la mise à jour, afin d'utiliser BitDefender. Un produit BitDefender qui constitue une mise à jour remplace le produit qui formait la base de votre éligibilité pour

la mise à jour. Vous pouvez utiliser le produit résultant seulement en accord avec les termes de cet Accord de licence. Si BitDefender est une mise à jour d'un composant d'un progiciel que vous avez acheté comme un seul produit, BitDefender peut être utilisé et transféré seulement comme une partie de ce progiciel et ne peut pas être séparé pour l'usage sur plus d'un ordinateur.

COPYRIGHT. Tous les droits d'auteur de BitDefender (comprenant mais ne se limitant pas à toutes les images, photographies, logos, animations, vidéo, audio, musique, texte et " applets " compris dans BitDefender), les matériels imprimés qui l'accompagnent et les copies de BitDefender sont la propriété de SOFTWIN. BitDefender est protégé par les lois concernant le copyright et par les traités internationaux. C'est pourquoi vous devez traiter BitDefender comme tout autre matériel protégé par le copyright à l'exception du fait que vous pouvez installer BitDefender sur un seul ordinateur, vu que vous gardez l'original seulement pour archive. Vous ne pouvez pas copier les matériels imprimés qui accompagnent BitDefender. Vous devez produire et inclure toutes les notices de copyright dans leur forme originale pour toutes les copies respectives du média ou de la forme dans laquelle BitDefender existe. Vous ne pouvez pas céder la licence, louer sous quelque forme que ce soit tout ou partie du logiciel BitDefender. Vous ne pouvez pas décompiler, désassembler, modifier, traduire ou tenter de découvrir le code source de ce logiciel ou créer des outils dérivés de BitDefender.

GARANTIE LIMITÉE. SOFTWIN garantit que le support sur lequel le logiciel est distribué est exempt de vices de matériaux et de fabrication pendant une période de trente (30) jours à compter de la date de livraison du logiciel. Votre seul recours en cas de manquement à cette garantie sera le remplacement par SOFTWIN du support défaillant durant la période de trente (30) jours à compter de la date de livraison du logiciel. SOFTWIN ne garantit pas que le logiciel répondra à vos besoins ni qu'il fonctionnera sans interruption ou sans erreur.

SOFTWIN REFUSE TOUTE AUTRE GARANTIE POUR BITDEFENDER, QUELLE SOIT EXPRESSE OU IMPLICITE. LA GARANTIE CI-DESSUS EST EXCLUSIVE ET REMPLACE TOUTES AUTRES GARANTIES, QU'ELLES SOIENT IMPLICITES OU EXPLICITES, Y COMPRIS LES GARANTIES IMPLICITES DE COMMERCIALISATION ET D'APPLICATION PARTICULIÈRE.

REFUS DES DOMMAGES. Toute personne qui utilise, teste ou évalue BitDefender admet les risques concernant la qualité et la performance de BitDefender. En aucun cas SOFTWIN ne sera tenu responsable à votre égard de tous dommages particuliers ou indirects, réclamations et pertes quelconques découlant de l'utilisation ou de l'incapacité d'utiliser le logiciel même si SOFTWIN a été avisé de l'éventualité de tels dommages.

NOTICE IMPORTANTE POUR LES UTILISATEURS. CE LOGICIEL N'EST PAS DÉSIGNÉ POUR DES MILIEUX DANGEREUX, DEMANDANT DES OPÉRATIONS OU UNE PERFORMANCE SANS ERREUR. CE LOGICIEL N'EST PAS RECOMMANDÉ DANS LES OPÉRATIONS DE NAVIGATION AÉRIENNE, INSTALLATIONS NUCLÉAIRES OU DES SYSTÈMES DE COMMUNICATION, SYSTÈMES D'ARMEMENT, SYSTÈMES ASSURANT DIRECTEMENT OU INDIRECTEMENT LE SUPPORT VITAL, CONTROLE DU TRAFFIC AÉRIEN, OU TOUTE AUTRE APPLICATION OU INSTALLATION OU LA DÉFAILLANCE POURRAIT AVOIR COMME EFFET LA MORT DES PERSONNES, DES BLESSURES PHYSIQUES SÉVÈRES OU DES DOMMAGES DE LA PROPRIÉTÉ.

RESTRICTIONS DE DROIT DU GOUVERNEMENT. Usage, duplication ou divulgation par le Gouvernement de BitDefender constituent sujet des restrictions stipulées par le sous paragraphe (c) (1) (ii) des Droits des Données Techniques et Software, clause DFARS 252.227-7013 ou sous paragraphes (c) (1) et (2) du Droit Commercial regardant le Software, clause 48 CFR 52.227-19. Contactez SOFTWIN au numéro 5,

rue Fabrica de Glucoza, 72 322 - Sect. 2, Bucarest, Roumanie ou au Tél. 40-21-2330780 ou Fax : 40-21-2330763.

CONDITIONS GÉNÉRALES. Cet accord est régi par les lois de la Roumanie et par les règlements et les traités internationaux concernant le copyright. Cet Accord peut être modifié par une annexe de licence qui accompagne cet Accord ou par un document écrit qui ait été signé par vous et par SOFTWIN. Les prix, les coûts et les frais d'usage de BitDefender peuvent changer sans que vous en soyez prévenu. Dans l'éventualité d'une invalidité de tout règlement de cet Accord, cette invalidité n'affectera pas la validité du reste de cet Accord. BitDefender et le logo de BitDefender sont des marques déposées de SOFTWIN. Microsoft, Windows, Excel, Word, le logo de Windows, Windows NT, Windows 2000 sont des marques déposées de la Corporation Microsoft. Toutes les autres marques appartiennent à leurs propriétaires respectifs.

2

Installation

Système requis

Pour assurer un fonctionnement correct du produit, vérifiez avant l'installation que vous disposez de la configuration suivante:

Processeur minimum : Pentium 200MHz ou compatible ;
Espace disque minimum : 40 Mo ;
Mémoire vive minimale : 64MB (128 Mo recommandés) ;
Système d'exploitation : Windows 98/NT-SP6/ME/2000/XP; Internet Explorer 4.0 (+) ;
Pour intégration de l'antispam dans la messagerie : Outlook Express 5.0 ou plus avancé, Microsoft Outlook 2000 ou plus avancé.

Etapes d'installation

Introduisez votre CD dans le lecteur. Un écran d'accueil vous proposera d'installer BitDefender. Cliquez sur cette option.
Si vous avez acheté le produit par téléchargement, localisez le fichier d'installation et double-cliquez dessus avec la souris.
Dans les deux cas, cela lancera l'assistant d'installation, qui vous guidera à travers le processus d'installation.

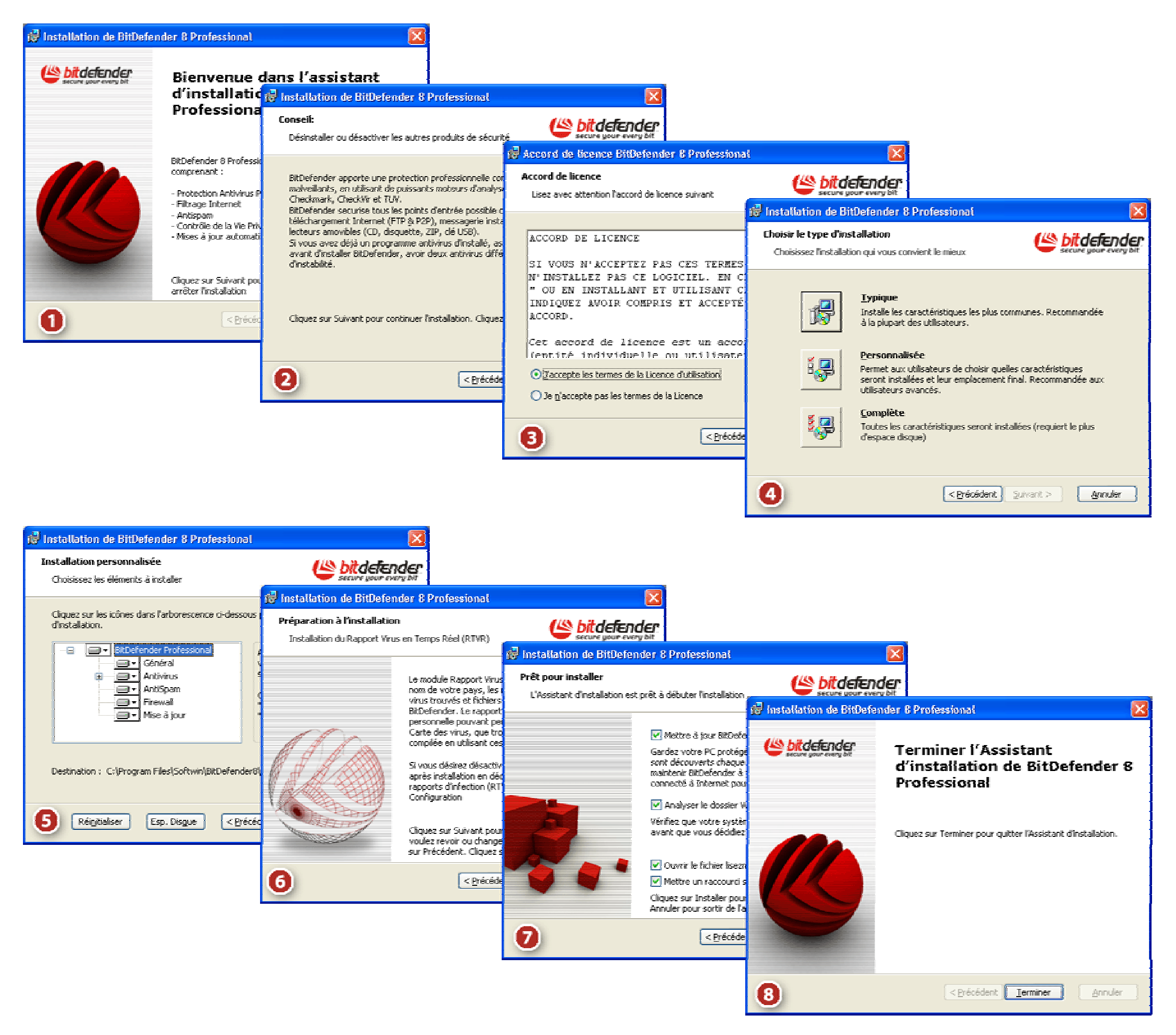


Figure 1

Etapes d'installation:

1. Cliquez sur **Suivant** pour continuer ou sur **Annuler** si vous voulez quitter l'installation.
2. Cliquer sur **Suivant** pour continuer ou sur **Retour** pour revenir à la première étape.
3. Merci de lire l' **Accord de Licence**, sélectionnez **J'accepte les termes de l'Accord de Licence** et cliquez sur **Suivant**. Si vous n'acceptez pas ces conditions, sélectionnez **Je n'accepte pas les termes de l'Accord de Licence** et cliquez sur **Annuler**. Le processus d'installation sera abandonné et vous sortirez de l'installation.
4. Vous pouvez choisir quel type d'installation vous souhaitez : typique, personnalisée ou complète.

   - **Typique** – Le programme sera installé avec les options les plus communes. Cela est recommandé pour la plupart des utilisateurs.
   - **Personnalisée** – Cela vous donne la possibilité de choisir les composants que vous souhaitez installer. Recommandé pour les utilisateurs « avancés » uniquement.
   - **Complète** – Pour l'installation complète du produit. L'ensemble des modules BitDefender seront installés.

   Si vous choisissez **typique** ou **complète** vous ne passerez pas par l'étape 5.

5. Si vous avez sélectionné **Personnalisé** une nouvelle fenêtre apparaîtra, contenant la liste de tous les composants de BitDefender afin de pouvoir choisir ceux que vous souhaitez installer.

Si vous cliquez sur l'un des composants, une courte description (incluant l'espace disque nécessaire) s'affichera sur le côté droit. Si vous cliquez sur un menu apparaîtra avec la possibilité de choisir d'installer ou non le module sélectionné.

Vous pouvez sélectionner le répertoire dans lequel installer le produit. Le répertoire par défaut est `C:\Program Files\Softwin\BitDefender 8`.

Si vous voulez choisir un autre répertoire, cliquez sur **Parcourir** et, dans la fenêtre qui s'ouvre, choisissez le répertoire. Cliquer sur **Suivant**.

6. Cliquez sur **Suivant**.

7. Vous avez quatre options sélectionnés par défaut:

   - **Mise à jour BitDefender** – pour mettre à jour BitDefender à la fin de l'installation. Votre système doit être connecté à Internet pour cela.
   - **Lancer une analyse complète du système** – pour rechercher des virus sur le PC à la fin de l'installation.
   - **Ouvrir le fichier lisezmoi** – pour ouvrir le fichier lisezmoi à la fin de l'installation.
   - **Créer un raccourci sur le bureau** – pour mettre un raccourci sur le bureau à la fin de l'installation.

   Cliquez sur **Installer** afin de commencer l'installation du produit.

8. Cliquez sur **Terminer** pour compléter l'installation du produit. Si vous avez accepté les paramétrages par défaut pour le répertoire d'installation, un nouveau répertoire du nom de **Softwin** est créé dans **Program Files**, contenant un sous-répertoire **BitDefender 8**.



Note

Il vous sera peut être demandé de redémarrer votre système pour terminer le processus d'installation.

Supprimer, réparer ou modifier les fonctions de BitDefender 8 SpamDeny

Si vous voulez modifier, réparer ou supprimer **BitDefender 8 SpamDeny**, suivez le chemin depuis le menu Démarrer de Windows: **Démarrer** → **Programmes** → **BitDefender 8** → **Modifier, reparer ou desinstaller**.

Il vous sera demandé confirmation de votre choix en cliquant sur **Suivant**. Une nouvelle fenêtre apparaîtra dans laquelle vous pourrez choisir:

- **Modifier** – pour sélectionner de nouveaux composants du programme à ajouter ou pour sélectionner des composants déjà installés et à retirer.
- **Réparer** – pour réinstaller tous les composants choisis lors de l'installation précédente.



Avant de réparer le produit, nous vous recommandons d'exporter vos listes d'Amis et de Spammeurs afin de les importer après la fin du processus de réparation.

- **Supprimer** – pour supprimer tous les composants installés.

Pour continue le processus, sélectionnez l'une des trois options listées ci-dessus. Nous recommandons **Supprimer** pour refaire une installation. Après la désinstallation, supprimez le sous-répertoire **Softwin** dans le répertoire **Program Files** pour assurer une nouvelle installation propre.

3

Description du produit

Description

Un bon logiciel antivirus ne suffit plus malheureusement tout seul dans un réseau. Les menaces informatiques ne proviennent pas seulement des virus, mais aussi des individus tels les hackers et les spammeurs. L'équipe de développement BitDefender reconnaît que le milieu informatique présent comporte beaucoup de risques, c'est pourquoi elle vient de créer un paquet de logiciels de sécurité.

BitDefender 8 SpamDeny intègre des modules antivirus, pare-feu et antispam dans un paquet de logiciels de sécurité, spécialement conçu pour les besoins des utilisateurs Internet, individuels ou entreprises.

Principales fonctions

BitDefender 8 SpamDeny inclut 3 modules de protection: **Antispam, Antivirus** et **Mise à jour**.

Antispam

Le module BitDefender Antispam gère votre problème de spam pour vous éviter de le faire vous-même.

Schéma de fonctionnement Antispam

Protection avancée Antispam
Le moteur Antispam BitDefender contient 5 filtres différents vous protégeant contre le spam: Liste d'amis / de spammeurs, Filtre jeu de caractères, Filtre d'Image, Filtre URL, Filtre heuristique, Filtre Bayesien.

Filtre bayesien avec auto-formation
Le filtre bayesien avancé qui apprend tout seul vous laisse classifier les messages en "Spam" ou "Non-spam", avec un seul clic. Le filtre commence apprendre après juste quelques répétitions, et vous vous retrouverez prenant de moins en moins de décisions avec le temps. Chaque étiquette que vous mettez améliore la précision du filtre. La sensibilité de votre filtre peut être haute ou réduite.

Sans soucis
Vous serez seulement notifiés sur réception des messages légitimes. Le spam sera collecté silencieusement dans votre dossier "spam" pour examination ultérieure.

Compatible avec tout client de messagerie

BitDefender Antispam fonctionne avec tous les clients de messagerie et peut être configuré de la console d'administration de BitDefender. De plus, il s'intègre avec Outlook et Outlook Express permettant une intéraction plus facile.

Antivirus

La mission du module AntiVirus est d'assurer la détéction et la désinfection de tous les virus en liberté. BitDefender Antivirus utilise des moteurs avancés d'analyse, certifiés par **ICSA Labs**, **Virus Bulletin, Checkmark, Checkvir** et **TUV**.

Quarantaine et rapports

Les fichiers suspicieux/infectés peuvent être aussi archivés dans une zone de quarantaine avant d'être désinfectés ou effacés. Le contenu de la quarantaine peut être envoyé aux laboratoires BitDefender, pour une analyse plus détaillée. Les fichiers non-infectés peuvent être remis facilement à leur place initiale.

Mise à jour

Celui-ci est le module qui effectue la mise à jour du produit avec de nouvelles signatures virales et nouvelles options.

Mises à jour rapides, gratuites et automatiques

Mise à jour intelligente de la protection antivirus, ne nécessitant pas l'intervention de l'utilisateur. La mise à jour peut être faite à partir du réseau, directement de l'Internet ou par un serveur proxy. Les possesseurs des licences BitDefender bénéficient des mises à jour gratuites des définitions virales et du produit.

Auto-réparation

Le produit est capable de se réparer tout seul si nécessaire, en téléchargeant les fichiers endommagés ou manquants à partir des serveurs de BitDefender.

Mise à jour automatique

Les mises à jour de l'antispam et de l'antivirus sont gratuites et automatiques. Les vérifications pour les nouvelles mises à jour peuvent être programmées aussi souvent que nécessaire.

Autres caractéristiques

Aide à la décision

Les assistants de configuration vous guideront à travers les étapes à suivre pour sécuriser votre système. Enfin, BitDefender vous informera directement sur votre bureau, dans une fenêtre discrète, de différentes alertes sur l'état de votre produit (mise à jour, date de dernière analyse…).

Facile à installer et à utiliser

Un assistant extrêmement intuitif vous guide à travers le processus d'installation. Une interface simple et amicale vous facilite l'utilisation du produit.

Support technique professionnel 24/24 – 7/7

Assuré par des personnes compétentes et une base de données en ligne qui répond aux questions les plus fréquemment posées.

4

La console de contrôle

Vue d'ensemble

BitDefender 8 SpamDeny a été conçu avec une console de management (gestion) centralisée, qui permet la configuration des options de protection de chaque module BitDefender. Autrement dit, il suffit d'ouvrir la console pour accéder aux différents modules: **Antispam**, **Antivirus** et **Mise à jour**.

L'accès à cette console se fait par le menu Démarrer de Windows, en suivant le chemin suivant: **Démarrer** → **Programmes** → **BitDefender 8** → **BitDefender 8 SpamDeny** ou plus rapidement en double-cliquant sur l'icône BitDefender dans la zone de notification (en bas à droite à côté de l'horloge).



Figure 2

Sur la partie gauche de la console, vous pouvez sélectionner les modules suivants:

- Général – pour accéder à la section résumant les principaux paramétrages de BitDefender, des informations produits et contacts. Vous pouvez également enregistrer le produit à cet endroit.
- Antivirus – pour accéder à la fenêtre de configuration de l'antivirus.
- Antispam – pour accéder à la fenêtre de configuration de l'antispam.
- Mise à jour – pour accéder à la fenêtre de configuration des mises à jour.

L'option **Plus d'infos**, placée en bas à droite ouvre la section **Aide**.

Lorsque la console est réduite, une icône apparaît dans le zone de notification.



Figure 3

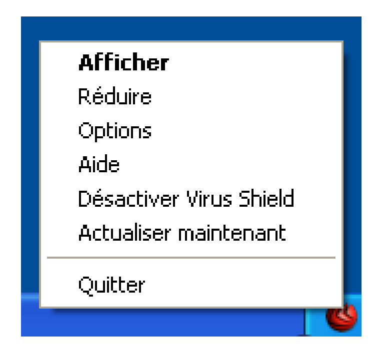


Figure 4

Si vous double-cliquez sur cette icône, la console s'ouvre.

De plus, en faisant un clic-droit dessus, comme dans la *Figure 7*, un menu contenant les options suivantes, apparaîtra.

- **Afficher** - ouvre la console de contrôle.
- **Réduire** - minimise la console, si elle est ouverte.
- **Options** - ouvre une fenêtre avec les options de la console.
- **Aide** - ouvre la documentation électronique.
- **Actualiser maintenant** – réalise une mise à jour immédiate.
- **Quitter** – ferme l'application. En choisissant cette option, l'icône dans la zone de notification disparaîtra. Pour la faire apparaître de nouveau, vous devrez la lancer depuis le menu **Démarrer**.

 **Note**

Si vous désactivez une ou plusieurs des modules BitDefender, l'icône sera grisée. Ainsi vous saurez si quelques modules sont désactivés sans ouvrir la console de gestion.
L'icône va clignoter si une mise à jour est disponible.

Module Général

BitDefender est par défaut paramétré pour une sécurité optimale. Les informations essentielles sur les modules de BitDefender sont affichées dans le module **Général**.

Il contient 4 sections différentes: Etat, Enregistrer, Configuration et A propos.

Etat

Vous pouvez consulter ici les informations concernant les status du produit.

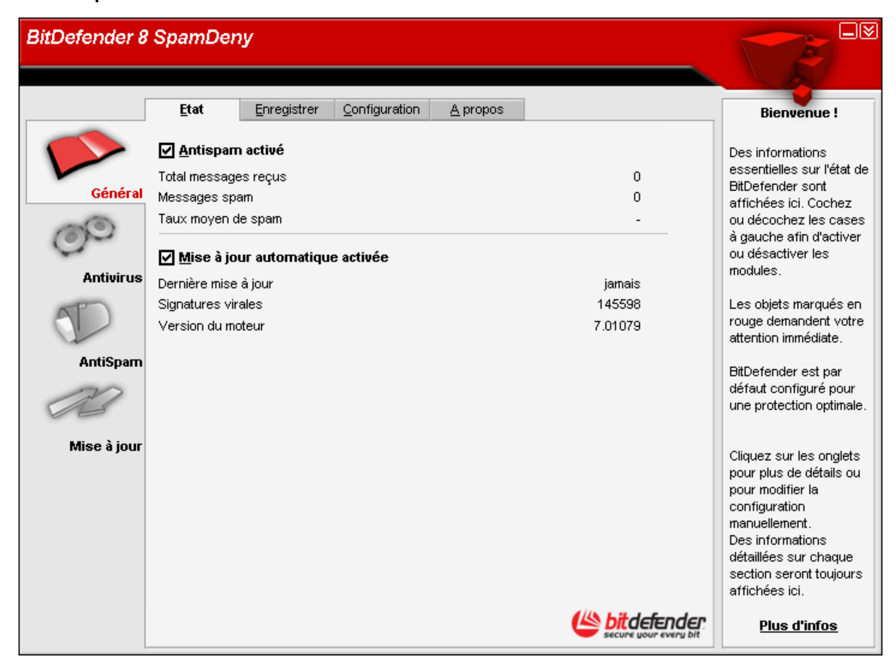


Figure 5

En cochant ou décochant les cases, vous pouvez activer ou désactiver certaines des principales fonctions de BitDefender.



Les points marqués en rouge nécessitent votre attention immédiate.

Antispam

Le Spam (courrier indésirable) est un problème croissant, à la fois pour les particuliers et pour les sociétés. Il y en a de nombreux types et formes différentes. BitDefender fonctionne avec tous les clients de messagerie et peut être configuré depuis la console de management (section Antispam). De plus il s'intègre directement dans Microsoft Outlook / Outlook Express une interaction précise avec le filtre AntiSpam à travers une interface intuitive et simple d'utilisation.



Pour prévenir l'arrivé de spam dans votre boîte aux lettres, laisser le filtre **Antispam** activé.

Voir comment BitDefender Antispam fonctionne

Mise à jour automatique

De nouveaux virus sont identifiés chaque jour. C'est pourquoi il est très important de garder BitDefender à jour avec les dernières signatures de virus. Cette rubrique affiche la date de dernière mise à jour et le nombre de virus détectables par votre version de BitDefender.



Pour protéger vos données critiques, BitDefender peut réaliser des mises à jour automatiques. Laissez l'option **Mise à jour Automatique** activé.

Enregistrement du produit

Cette section contient des informations sur le statut de vos licences BitDefender. Vous pouvez ici enregistrer votre produit et voir sa date d'expiration.

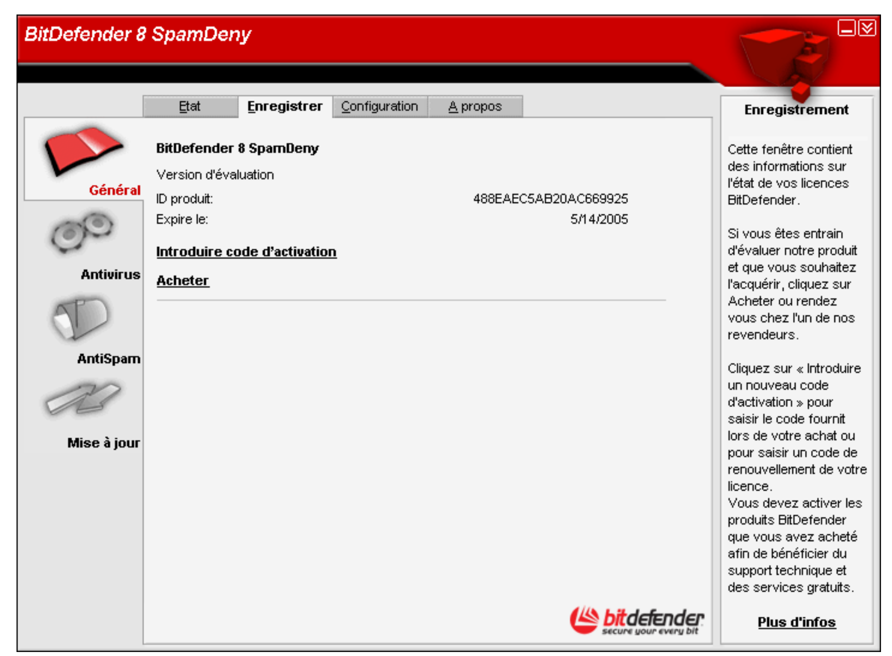


Figure 6

Cette section contient des informations sur le statut de vos licences BitDefender. Vous pouvez ici enregistrer votre produit et voir sa date d'expiration.

Le produit est livré par défaut avec un code d'évaluation valable 30 jours. A la fin de cette période d'essai, si vous souhaitez acheter le produit, vous pouvez cliquer sur le bouton **Acheter** ou vous rendre chez l'un de nos revendeurs.

Pour modifier la licence par défaut, cliquez sur **Introduir code d'activation**. La fenêtre suivante apparaîtra:

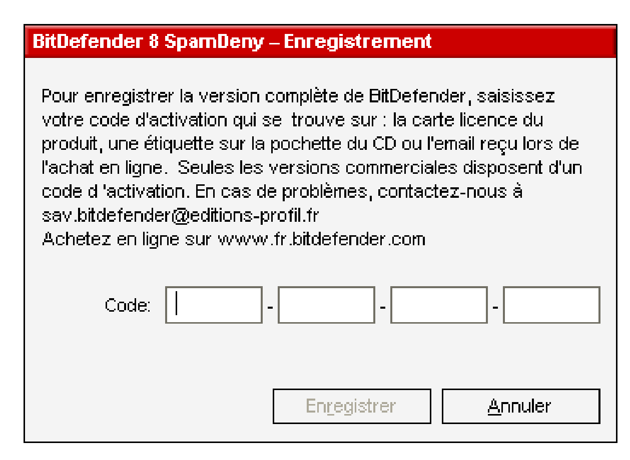


Figure 7

Saisissez votre code dans le champ **Code** et cliquez sur **Enregistrer** pour finir l'enregistrement.

Si vous faîtes une erreur de saisie, il vous sera demandé de la re-rentrer.

Si vous entrez un code d'activation valide, une boîte de dialogue vous le confirmera.

Dans la section **Enregistrement**, vous pourrez voir à présent la date d'expiration de votre nouveau code d'activation.

Astuce: Merci d'activer le produit BitDefender que vous avez acheté pour pouvoir bénéficier du support technique et des services BitDefender.

Paramétrages de la console de contrôle

Vous pouvez dans cette rubrique paramétrer le fonctionnement de BitDefender. Par défaut, BitDefender est chargé au démarrage de Windows et se réduit automatiquement.

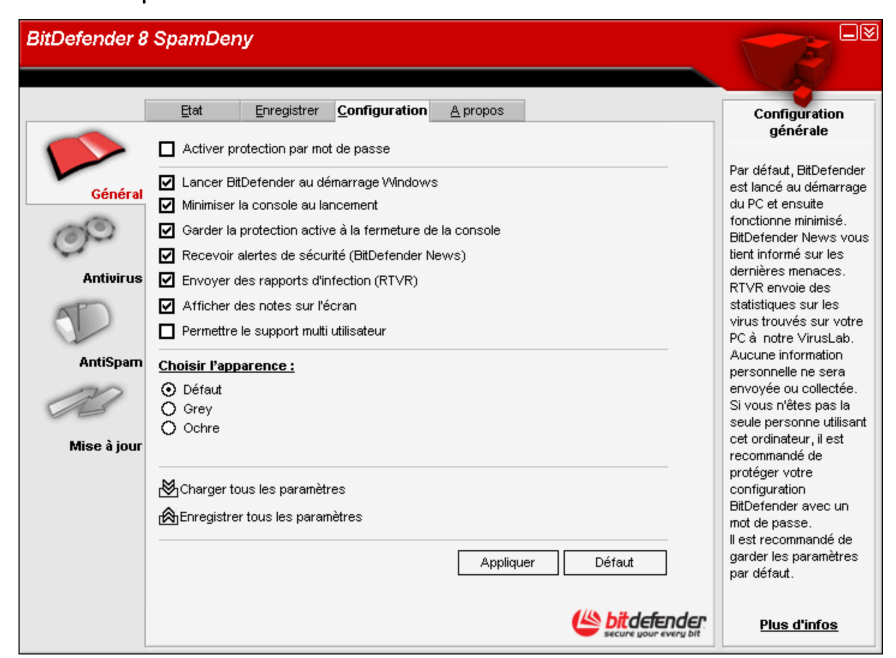


Figure 8

Pour choisir une option, cliquez simplement sur la case correspondante.

➔ **Activer protection par mot de passe** – permet de choisir un mot de passe afin de protéger la configuration choisie pour BitDefender.



Si vous n'êtes pas le seul utilisateur de votre ordinateur, il est recommandé de protéger vos paramétrages BitDefender par un mot de passe.

La fenêtre suivante apparaîtra:

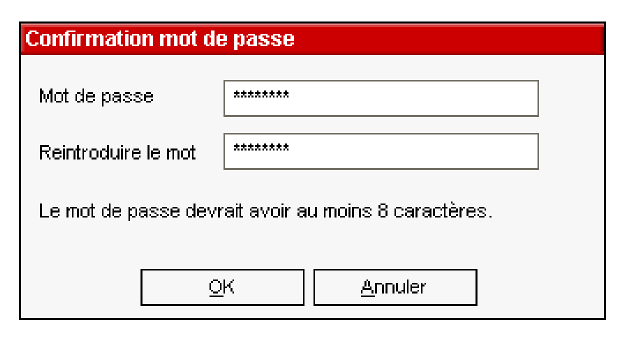


Figure 9

Entrez le mot de passe dans le champ **Mot de passe**, re-saisissez le dans le champ **Reintroduire le mot** de passe et cliquez sur **OK**.

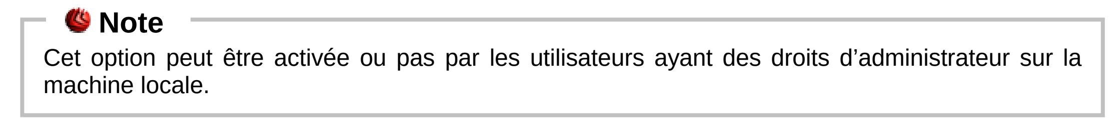
A présent, si vous souhaitez changer les options de configuration de BitDefender, le mot de passe vous sera demandé.



Si vous oubliez le mot de passe, vous devrez réparer le produit afin de pouvoir modifier la configuration de BitDefender.

- **Lancer BitDefender au démarrage Windows** – lance automatiquement BitDefender au démarrage du système. Cela est fortement recommandé!
- **Minimiser la console au lancement** – réduit la console de management BitDefender après son chargement au démarrage. Seul l'icône BitDefender apparaîtra dans la zone de notification.
- **Garder la protection à la fermeture de la console** – même si la console est fermée (plus apparente dans la zone de notification), BitDefender continuera à vous protéger.
- **Recevoir alertes de sécurité** – affiche régulièrement des informations de sécurité sur des risques de virus et/ou de failles, envoyées par serveurs de BitDefender.
- **Afficher l'écran d'accueil**– montre l'écran qui apparaît lorsque vous lancez BitDefender.
- **Envoyer des rapports d'infection**– envoie au laboratoire BitDefender des rapports concernant les virus identifiés sur vote PC.

  Le rapport ne contiendra aucune donnée confidentielle, comme votre nom, votre adresse IP ou autre et ne sera pas utilisé à des fins commerciales. Les informations envoyées contiendront seulement le nom des virus et seront utilisées pour créer des rapports statistiques.
- **Afficher des notes sur l'écran** – affiche des fenêtres d'alertes sur les statuts de votre produit.
- **Permettre le support multi utilisateur** – permet aux autres utilisateurs du même ordinateur de garder leur configuration pour BitDefender.



Note

Cet option peut être activée ou pas par les utilisateurs ayant des droits d'administrateur sur la machine locale.

- L'option **Choisir l'apparence** vous permet de sélectionner la couleur de la console de management. Le skin représente l'image de fond de l'interface. Pour sélectionner un skin différent, cliquez sur la couleur correspondante.

Utilisez les boutons **Sauvegarder Tous les paramètres** / **Charger Tous les Paramètres** pour sauvegarder ou charger les paramètres établis pour BitDefender dans un endroit spécifié. Ainsi, vous pouvez utiliser les mêmes paramètres après la réinstallation ou la réparation de votre BitDefender.

Cliquez sur **Appliquer** pour enregistrer les modifications. Si vous cliquez sur **Défaut** vous allez charger les paramètres par défaut.

A propos

Dans cette section vous pouvez trouver des informations sur votre produit et les contacts dont vous pourriez avoir besoin.

BitDefender^{TM} fournit des solutions de sécurité pour satisfaire les besoins de protection des environnements informatiques actuels et protège actuellement plus de 120 millions d’utilisateurs particuliers ou professionnels dans plus de 100 pays.

BitDefender^{TM} est certifié par tous les principaux organismes de tests indépendants - **ICSA Labs**, **CheckMark**, **Virus Bulletin** et **TUV**, et est la seule solution de sécurité à avoir reçu le prix européen de l’innovation technologique **IST Prize**.

Module Antivirus

L'objectif principal de BitDefender est de conserver votre PC sans virus. Cela est assuré avant tout par l'analyse antivirus des emails que vous recevez et des fichiers que vous téléchargez ou copiez sur votre système.

Plus de fonctions

Il y a cependant un risque qu'un virus soit déjà logé dans votre système, avant même l'installation de BitDefender. C'est pourquoi il est prudent d'analyser votre ordinateur après l'installation de BitDefender et c'est encore plus prudent d'analyser régulièrement votre ordinateur contre les virus.

BitDefender permet quatre types d'analyse à la demande:

- Analyse immédiate – il y a quelques étapes à suivre pour analyser votre ordinateur contre les virus;
- Analyse contextuelle – un clic-droit sur un fichier ou répertoire permet de sélectionner **BitDefender Antivirus v8**;
- Analyse programée – vous pouvez programmer BitDefender pour analyser votre système contre les virus périodiquement.

Analyse immédiate

Pour analyser votre ordinateur contre les virus, veuillez suivre les étapes suivantes:

1. Fermez tous les programmes ouverts

Afin de permettre à BitDefender de réaliser une analyse complète, il est nécessaire de fermer tous les programmes ouverts, tout spécialement les clients de messagerie (ex : Outlook, Outlook Express ou Eudora).

2. Vérifiez que BitDefender est à jour contre les derniers virus

Avant de laisser BitDefender analyser votre ordinateur, vous devriez vérifier que BitDefender est à jour de ses signatures de virus, dans la mesure où de nouveaux virus apparaissent chaque jour. Vous pouvez vérifier de quand date la dernière mise à jour en bas du module Mise à jour de la **console de management BitDefender**.

Si cette date n'est pas récente, vous devriez laisser BitDefender mettre à jour ses signatures de virus. C'est très simple, tout ce que vous avez à faire et de cliquez sur le bouton **Vérification** dans le module Mise à jour.

3. Choisissez la cible de l'analyse

Dans la console de management, entrez dans le module Antivirus et cliquez sur l'onglet Analyse. Par défaut, la section contient une image de la structure des partitions du système. A côté de cela, des boutons et options d'analyse peuvent également être observés.

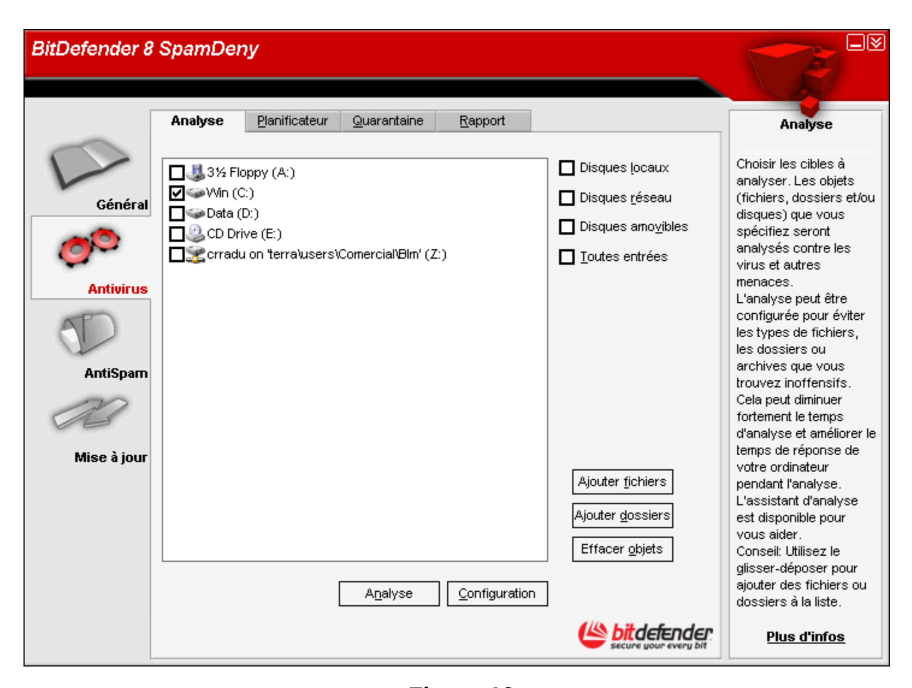


Figure 10

La section contient les boutons suivants:

➔ **Ajouter fichiers** - le bouton qui permet de rajouter des fichiers pour l'analyse. En cliquant dessus, une fenêtre de navigation s'ouvre et vous pouvez choisir le fichier.

➔ **Ajouter dossiers** - le bouton qui permet de rajouter un nouveau dossier pour l'analyse. En cliquant dessus, une fenêtre de navigation s'ouvre et vous pouvez choisir le dossier.

Astuce: Vous pouvez rajouter des fichiers et des dossiers à la liste d'analyse en les glissant-déposant sur la section **Analyse**.

➔ **Effacer sélection** - efface le fichier/dossier sélectionné auparavant.


Seulement les fichiers/dossiers rajoutés après peuvent être effacés, mais pas ceux qui sont automatiquement "proposés" par BitDefender.

➔ **Paramétrages** – ouvre une fenêtre dans laquelle vous pouvez spécifier quels types de fichiers sont à analyser, l'action sur les fichiers infectés, la génération de messages d'alertes, la sauvegarde des résultats d'analyse dans des fichiers rapports.

➔ **Analyse** - lance l'analyse en tenant compte des options choisies.

Ces options permettent une sélection rapide des cibles d'analyses:

- **Disques locaux** – pour analyser les disques locaux.
- **Disques réseaux** – pour analyser tous les lecteurs réseaux.
- **Disques amovibles** – pour analyser les disques amovibles (CD-ROM, lecteur de disquettes).
- **Toutes les entrées** – pour analyser l'ensemble des lecteurs, peu importe qu'ils soient locaux, réseaux ou amovibles.

Si vous voulez analyser l'ensemble de votre ordinateur, cochez la case **Toutes les entrées**.

Si vous n'êtes pas habitué à paramétrer, vous pouvez à présent cliquer sur le bouton **Analyse**. BitDefender commencera l'analyse de votre PC avec les paramétrages standard, qui sont suffisants.

4. Sélectionnez les options d'analyse – seulement pour les utilisateurs avancés

Les utilisateurs avancés peuvent vouloir tirer avantage des possibilités de paramétrage d'analyse de BitDefender. Le scanner peut être paramétré pour éviter certaines extensions de fichiers, répertoires ou archives que vous savez être sans danger. Cela peut considérablement réduire le temps d'analyse et améliorer le temps de réaction de votre ordinateur durant une analyse.

Explorez cela en cliquant sur l'onglet **Configuration**.

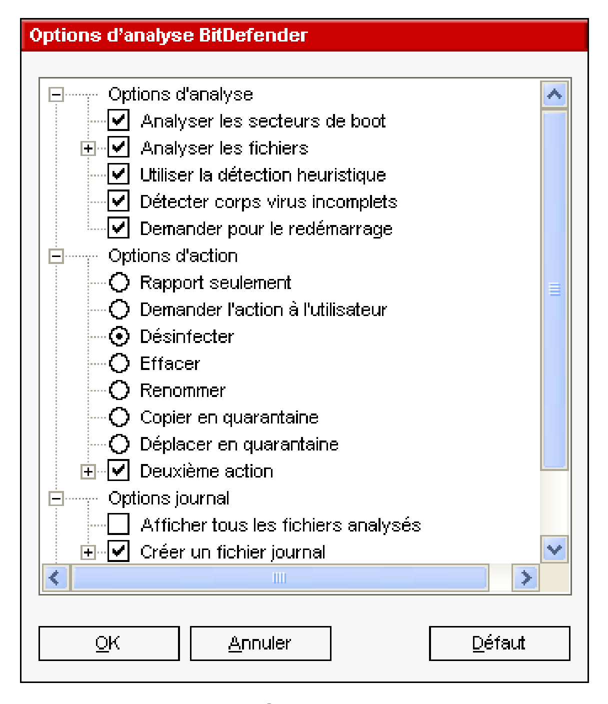


Figure 11

Les options d'analyse sont organisés en menus extensibles très proche de ceux qui sont utilisés dans l'explorateur Windows.

Les options d'analyse sont groupées en quatre catégories:

- **Options d'analyse**
- **Options d'action**
- **Options jurnal**
- **Options de performance**

Cliquez sur la case avec un "+" pour ouvrir une option et sur la case avec un "-" pour fermer une option.

L'étape suivante permet de spécifier le type d'objets à analyser (archives, e-mail et autres) et permet d'activer l'analyse heuristique (pour détecter des virus encore inconnus). Cela est réalisé par la sélection de certaines options dans la catégorie **Options d'analyse**.

Les options suivantes sont disponibles:

Option		Description
Analyser les secteurs de boot		Pour analyser les secteurs de boot du système.
Analyser les fichiers	Analyser tous les fichiers	Pour analyser tous les fichiers, quelque soit leur type.
	Analyser seulement les extensions à risques	Pour analyser seulement les fichiers avec les extensions suivantes: `exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pfd; msi; ini; csc; cmd; bas; eml; nws.`
	Analyser les extensions définies par l'utilisateur	Pour analyser seulement les fichiers avec les extensions définies par l'utilisateur. Ces extensions doivent être séparées par ";".
	Exclure les extensions définies par l'utilisateur	Pour analyser tous les fichiers, à l'exception de ceux avec des extensions définies par l'utilisateur. Ces extensions doivent être séparées par ";".
	Ouvrir les paquets programmes	Analyser les fichiers en paquets.
	Ouvrir les archives	Analyser l'intérieur des archives.
	Ouvrir les archives des messagerie	Analyser dans les archives de messagerie.
Utiliser la détection heuristique		Active l'analyse heuristique des fichiers. Le but de l'analyse heuristique est d'identifier de nouveaux virus, se basant sur des algorithmes spécifiques, avant que ces virus soient connus. De fausses alertes peuvent apparaître et cette méthode ne peut pas garantir un taux de détection à 100% de ces nouveaux virus. Quand un tel fichier est détecté il est classifié comme étant suspect. Dans ce cas, nous vous recommandons d'envoyer le fichier au laboratoire BitDefender afin qu'il soit analysé.

Ensuite vous devez spécifier **l'action à appliquer aux fichiers suspects et infectés**. L'action peut être sélectionnée dans la catégorie **Options d'action**. Cliquez sur le "+" pour l'ouvrir et voir toutes les actions possibles sur les fichiers infectés.

Vous pouvez sélectionner l'une des suivantes:

Action	Description
Rapport seulement	Pour rapporter la détection d'un fichier infecté et le nom du virus.
Demander l'action à l'utilisateur	Quand un fichier infecté est détecté, une fenêtre apparaît, demandant à l'utilisateur de choisir une action à appliquer au fichier. Suivant l'importance du fichier, vous pouvez choisir de le désinfecter, l'isoler en quarantaine ou l'effacer.
Désinfecter	Pour désinfecter les fichiers infectés.
Effacer	Pour effacer les fichiers infectés.
Renommer	Pour renommer les fichiers infectés.
Copier en quarantaine	Pour copier les fichiers infectés dans la zone de quarantaine. ! Cela revient concrètement à dupliquer le fichier infecté dans la zone de quarantaine, mais le fichier infecté ne sera pas retiré de son emplacement d'origine.
Déplacer en quarantaine	Déplacer les fichiers infectés dans la zone de quarantaine. ! Lorsque le virus est en quarantaine il ne peut faire aucun dégat.
Deuxième action	Cliquez sur cette option si vous désirez sélectionner la deuxième action à appliquer aux fichiers infectés. Ceci n'est possible que si la première action choisie est "Désinfecter".

Pour sélectionner la deuxième action à appliquer, cliquez sur le "+", après avoir coché **Deuxième action**.

Les options disponibles en deuxième action sont décrites dans le tableau ci-dessous.

Action	Description
Rapport seulement	Pour rapporter la détection d'un fichier infecté et le nom du virus.
Demander l'action à l'utilisateur	Quand un fichier infecté est détecté, une fenêtre apparaît, demandant à l'utilisateur de choisir une action à appliquer au fichier. Suivant l'importance du fichier, vous pouvez choisir de le désinfecter, l'isoler en quarantaine ou l'effacer.
Effacer	Pour effacer les fichiers infectés.
Renommer	Pour renommer les fichiers infectés.
Copier en quarantaine	Pour copier les fichiers infectés dans la zone de quarantaine. ! Cela revient concrètement à dupliquer le fichier infecté dans la zone de quarantaine, mais le fichier infecté ne sera pas retiré de son emplacement d'origine.
Déplacer en quarantaine	Déplacer les fichiers infectés dans la zone de quarantaine. ! Lorsque le virus est en quarantaine il ne peut faire aucun dégat.

L'étape suivante est la sélection des options journal. Vous devez cliquer sur le signe "+" correspondant aux **Options journal**. Ces options permettent l'activation des alertes et la création des fichiers journal (contenant des informations sur l'analyse).

Option		Description
Afficher tous les fichiers analysés		Affiche tous les fichiers, infectés ou pas, et leur état dans un fichier journal.
Créer un fichier journal	Nom du fichier rapport	Ceci est un champ qui permet le changement du nom du fichier rapport. Vous devez simplement cliquer sur cette option et introduire un nouveau nom.
	Ajouter au rapport existant	Choisissez cette option pour ajouter les informations sur la dernière analyse à la fin du journal, après celles déjà existantes.
	Limiter la taille du journal à [x] Ko	Cliquez sur cette option et introduisez la taille maximum du fichier dans le champ qui apparaît.

Dans la catégorie **Options de performance** vous pouvez décroître la priorité du processus d'analyse. Si vous cochez la case **Exécuter la tâche d'analyse avec une priorité basse** vous allez permettre aux autres logiciels d'être exécutés à une vitesse supérieure et d'augmenter le temps nécessaire pour le final du processus d'analyse.

Astuce: Vous pouvez voir le fichier de rapport dans la section Rapport du module **Antivirus**.

 **Note**

Vous pouvez observer que certaines options d'analyse, bien que le signe "+" apparaisse, ne peuvent s'ouvrir. La raison est que ces options n'ont pas encore été sélectionnées. Vous observerez que si vous les cochez, elles pourront être ouvertes.

Cliquez sur **OK** pour enregistrer les modifications. Si vous cliquez sur **Défaut** vous allez charger les paramètres par défaut.

5. Analyse virale

Une fois les options d'analyse choisies, tout ce qu'il vous reste à faire est de démarrer l'analyse. Pour le faire, cliquez sur **Analyse**. Cela peut durer un certain temps, suivant la taille de votre disque.

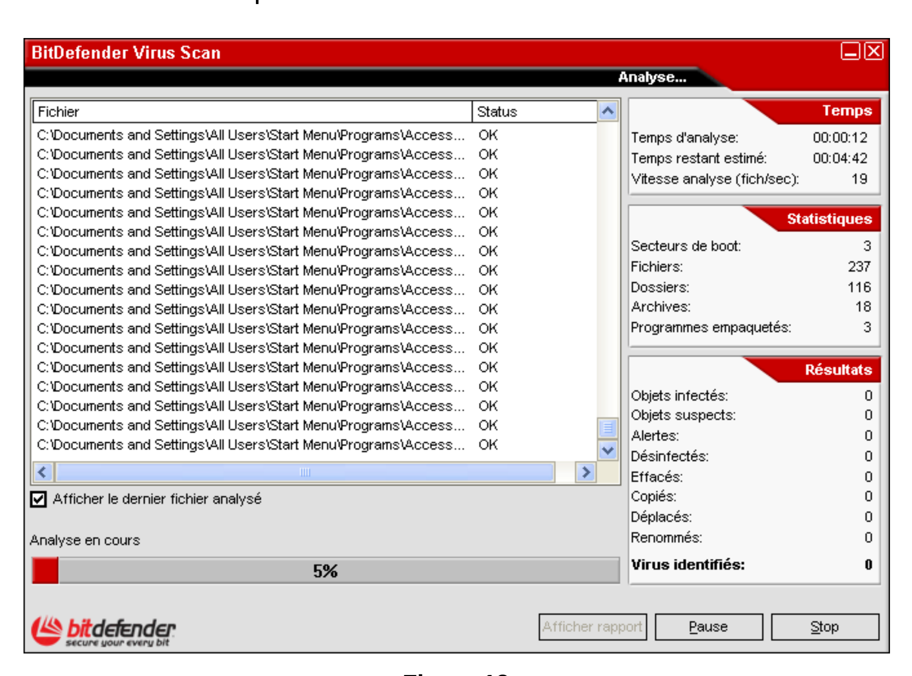


Figure 12

Durant l'analyse, BitDefender vous montrera sa progression et vous alertera si le moindre virus est trouvé.

Cochez la case correspondante à **Afficher le dernier fichier analysé** et seulement les informations sur les derniers fichiers analysés seront visibles.

Si vous cliquez:

- **Stop** - une nouvelle fenêtre s'affichera vous permettant de stopper la vérification du système. Si vous choisissez d'arrêter, le bouton **Stop** se transformera en un bouton **Fermer** et le chosir fermera la fenêtre d'analyse.
- **Pause** - l'analyse s'arrête temporairement – vous pouvez la continuer en cliquant sur **Poursuivre**.
- **Afficher le rapport** – le rapport d'analyse s'ouvre.

Le fichier rapport est sauvegardé automatiquement dans la section Rapport du module **Antivirus**.

Astuce: Afin de voir les fichiers analysés vous devez sélectionner l'option **Afficher tous les fichiers scannés** dans les options de rapport (étape précédente). Avec cette option activée, l'ordinateur sera ralentit.

6. Analyse contextuelle

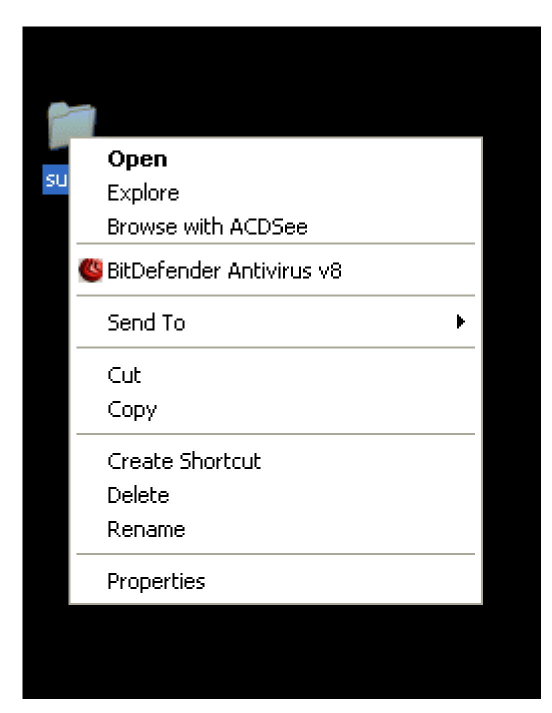


Figure 13

Faîtes un clic-droit sur le fichier ou répertoire que vous souhaitez analyser et sélectionnez l'option **BitDefender Antivirus v8**.

Un fichier rapport nommé `vscan.log` sera créé et accessible dans le module **Antivirus**, section Rapport.

Si un virus est détecté, une fenêtre d'alerte (Figure 24) apparaîtra:



Figure 14

Vous pouvez voir le nom du fichier et le nom du virus.

Vous pouvez sélectionner une des options suivantes:

- **Désinfecter** - désinfecter le fichier infecté.
- **Effacer** - effacer le fichier infecté.
- **Copier en** quarantaine – copier le fichier infecté dans la zone de quarantaine.
- **Déplacer en** quarantaine – déplacer le fichier infecté dans la zone de quarantaine.
- **Renommer** - pour renommer le fichier infecté.
- **Ignorer** - ignorer l'infection. Aucune action ne sera appliquée au fichier infecté.

Si vous analysez un répertoire, et que vous souhaitez que l'action sur les fichiers infectés soit la même pour tous, cochez l'option **Appliquer à tous**.



Si l'option **Désinfecter** n'est pas activée, cela veut dire que le fichier ne peut pas être désinfecter. Le meilleur choix est alors de l'isoler en quarantaine et de nous l'envoyer, ou de le supprimer.

A la fin, cliquez sur **OK**.

Analyse programmée

Etant donné que l'analyse prendra du temps, et qu'elle fonctionnera mieux si vous avez fermé les autres programmes, il est préférable pour vous de programmer une analyse à une heure où vous n'utilisez pas votre ordinateur. Cela implique que l'utilisateur doit à l'avance créer une tâche.

Les fonctions suivantes sont disponibles:

- Assistant de création de tâches d'analyses programmées;
- Sélection de la fréquence d'analyse;
- Sélection des lecteurs et/ou répertoires;
- Sélection des extensions de fichiers;
- Possibilité de configuration distincte pour chaque tâche d'analyse;
- Possibilité d'analyse réseau (LAN);
- Isolation automatique en zone de quarantaine des fichiers infectés ou suspects;
- Analyse en tâche de fond sans interférence avec l'activité de l'utilisateur;
- Sommaire des propriétés des tâches programmées;
- Création de rapports d'analyse.

Dans la console de management, entrez dans le module **Antivirus** et cliquez sur l'onglet **Planificateur**.

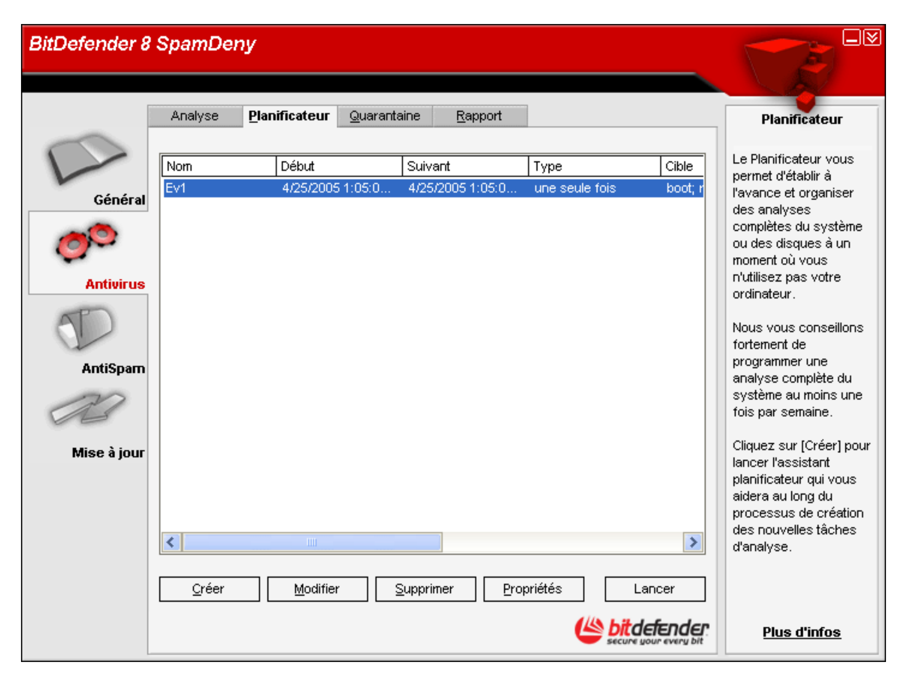


Figure 15

La section du **Planificateur** contient quelques boutons pour administrer les tâches d'analyse:

➔ Creér – lance l'assistant qui vous guidera dans la création d'une nouvelle tâche d'analyse.
➔ **Modifier** – modifie les propriétés d'une tâche précédemment créée. Cela lance également l'assistant.

Si vous modifiez le nom d'un évènement, un nouvel évènement sera créé, sous le nouveau nom saisi.

➔ **Supprimer** – efface une tâche sélectionnée.
➔ **Propriétés** – affiche les propriétés d'une tâche sélectionnée.
➔ **Lancer** – démarre immédiatement la tâche choisie.

L'écran du **Planificateur** contient également une liste où toutes les tâches peuvent être vues, avec leur nom, la date de première exécution, la date de la prochaine exécution et son type (périodique ou une fois seulement).

Le **Planificateur** intègre un assistant de création de nouvelles tâches d'analyse. Il vous assistera chaque fois que vous aurez besoin de faire une opération sur ces évènements, que ce soit pour créer une nouvelle tâche ou pour en modifier une existante.

Cliquez sur Creér. Cela lancera l'assistant de création de tâches.

Astuce: Nous vous recommandons fortement de programmer une analyse complète du système au moins une fois par semaine.

1. Spécifier le nom de la tâche

Il vous faut tout d'abord spécifier un nom pour la nouvelle tâche.

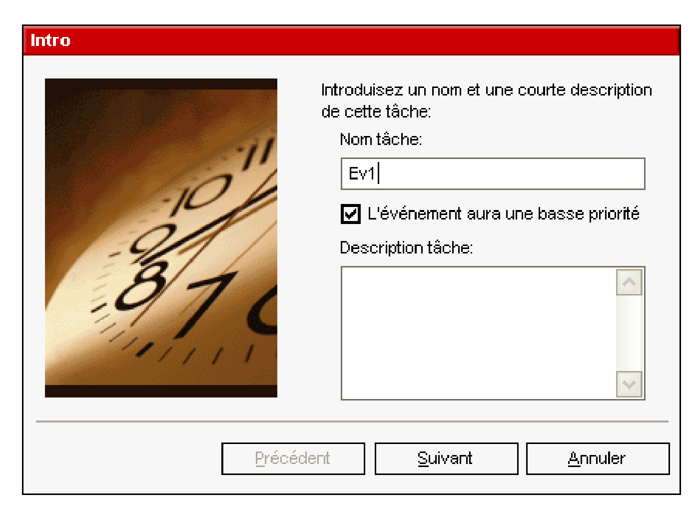


Figure 16

Tapez le nom du nouvel évènement dans le champ **Nom tâche** et un court descriptif dans le champ **Description tâche**.

Cochez la case **Lévénement aura une basse priorité** si vous désirez diminuer la priorité de la tâche d'analyse et permettre aux autres logiciels d'être exécutés plus rapidement. Cela augmentera le temps nécessaire pour la fin de la tâche.

Cliquez sur **Suivant** pour continuer. Si vous cliquez sur **Annuler** une fenêtre apparaîtra pour vous demander confirmation.

2. Sélectionner la fréquence d'analyse

Suite à cela, une fenêtre où vous pourrez sélectionner le type d'analyse s'affichera. Cochez la case **Une seule fois** si vous voulez programmer une analyse ponctuelle. Si vous souhaitez que l'analyse soit répétée après un certain intervalle, cochez la case **Périodiquement**.

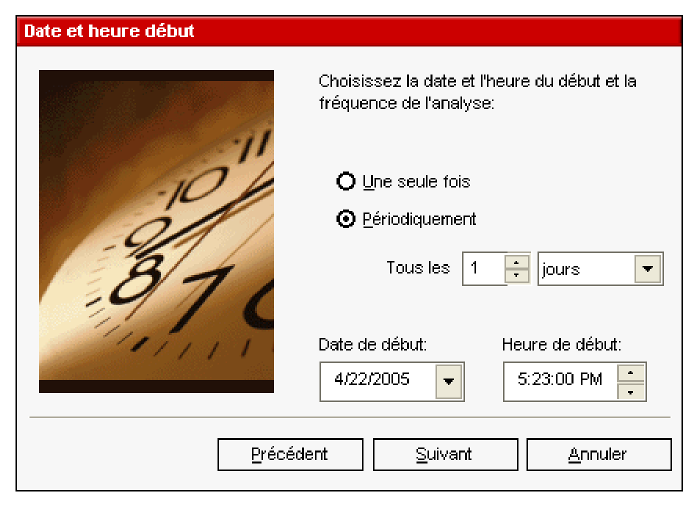


Figure 17

Tapez dans le champ **Tous les** le nombre de minutes / heures / jours / semaines / mois / années après lequel vous voulez répéter ce processus.

Vous pouvez cliquer sur les flèches de cette boîte afin d'augmenter / baisser le nombre de minutes / heures / jours / semaines / mois / années.

Sélectionnez l'intervalle - minutes, heures, jours, semaines, mois, années – après lequel l'analyse sera répétée. Faîtes défiler la liste et choisissez l'unité de temps souhaitée.

Si vous choisissez une analyse répétée, l'évènement sera lancé pour une période de temps illimitée. Afin de le stopper, il doit être effacé de la liste des évènements de la fenêtre du **Planificateur**.

Après avoir sélectionné la période, cliquez sur **Suivant** pour continuer. Si vous souhaitez revenir en arrière, cliquez sur **Précédent**.

3. Selection des objets à analyser

Cette étape permet de sélectionner les objets que vous souhaitez analyser – le secteur de boot, les fichiers, les archives, les fichiers en paquets.



Figure 18

Sélectionnez un ou plusieurs objets à analyser, en cochant simplement ceux que vous souhaitez.

Vous pouvez sélectionner les objets suivants:

- Boot – pour analyser le secteur de boot, afin d'identifier les virus de boot;
- **Fichiers** – pour analyser les fichiers;
- **Archive messagerie** – pour analyser les archives de mail;
- Archives – pour analyser à l'intérieur des archives;
- Paquets – pour analyser les fichiers en paquets.

Cliquez sur **Suivant**.

4. Sélection du chemin

Ici vous devez spécifier le répertoire des objets à analyser, comme observé sur la capture. Cette étape est nécessaire si vous avez sélectionné l'analyse de fichiers dans l'étape précédente.

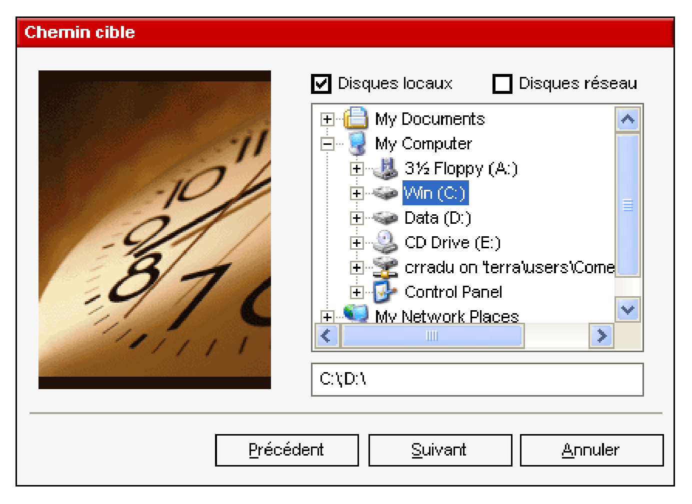


Figure 19

Cet écran est une fenêtre d'exploration qui vous permet de sélectionner les partitions et répertoires à analyser.

Lorsque le curseur est placé sur un répertoire, le chemin complet du répertoire apparaîtra dans le champ inférieur.

Cliquez sur la case “+" pour ouvrir une option ou sur celle "-" pour fermer une option.

Par ailleurs, pour sélectionner les éléments à analyser, vous pouvez utiliser les options de sélection rapide placées en haut de la fenêtre:

- **Disques locaux** - pour analyser tous les disques locaux;
- **Disques réseau** - pour analyser tous les disques du réseau.

Cliquez sur **Suivant**.

5. Sélection des types de fichiers

Spécifiez les types e fichiers à analyser.

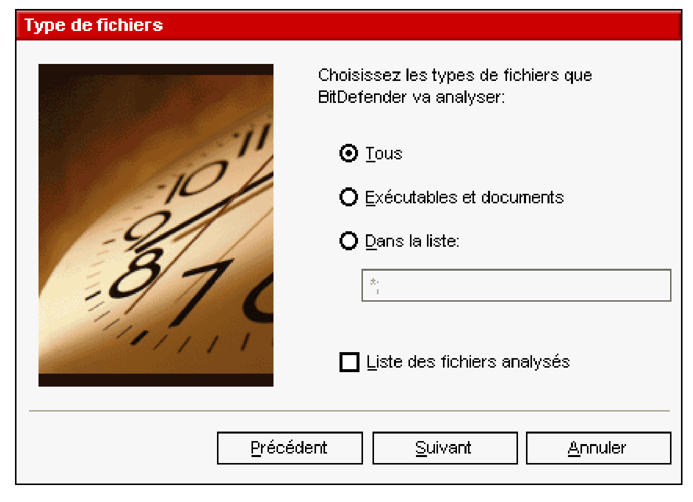


Figure 20

Cette étape est nécessaire seulement si vous avez sélectionné l'analyse de fichiers.

Vous pouvez sélectionner:

- **Tous** – pour analyser tous les fichiers, quel que soit leur type;
- **Exécutables et documents** – pour analyser les fichiers programmes et les documents;
- **Dans la liste** – pour analyser seulement les fichiers dont l'extension apparaît dans la liste. Ces extensions doivent être séparées par “;”.

Si vous souhaitez voir les informations sur l'ensemble des fichiers scannés, infectés ou non, sélectionnez l'option **Liste des fichiers analysés**.

Cliquez sur **Suivant**.

6. Sélection du type d'analyse

Sélectionnez le type d'analyse.

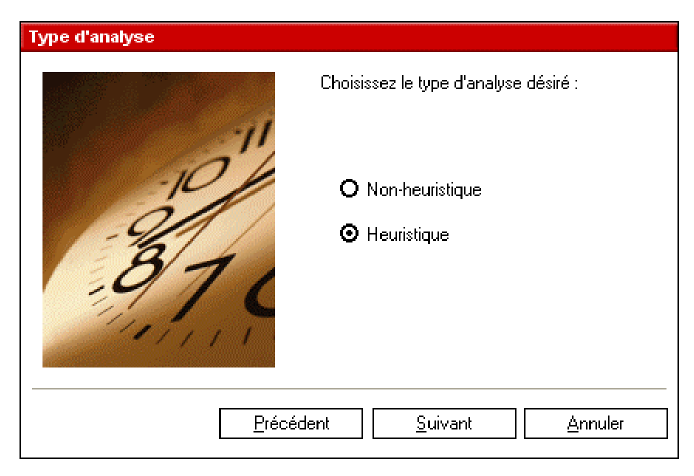


Figure 21

Cela, comme indiqué sur l'image, permet de sélectionner l'un des deux types d'analyse:

- **Analyse** Non-heuristique - analyse les fichiers avec une procédure basée sur des signatures de virus connus. Pour activer ce type d'analyse, sélectionnez **Non-Heuristique**;
- **Analyse** Heuristique – représente une méthode basée sur certains algorithmes, qui permettent d'identifier de nouveaux virus encore inconnus. Parfois, elle peut générer des rapports de codes suspects dans des programmes normaux, ce que l'on appelle des "false positive" (ou fausse alerte). Pour activer ce type d'analyse, sélectionnez **Heuristique**.

Cliquez sur **Suivant**.

7. Selection de l'action sur les fichiers infectés

BitDefender permet de choisir deux actions dans le cas où des fichiers infectés sont trouvés.

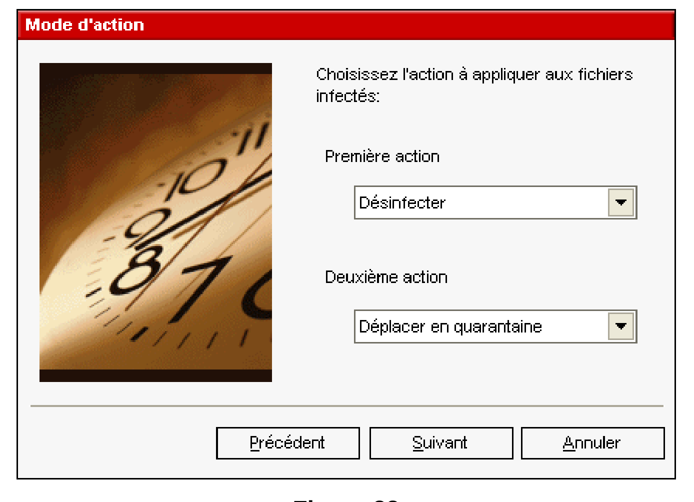


Figure 22

Nous vous recommandons de sélectionner **Désinfecter** en première action et **Déplacer en Quarantaine** en seconde action.

Vous pouvez sélectionner l'une des actions suivantes pour la première action:

Action	Description
Désinfecter	Pour désinfecter les fichiers infectés.
Effacer	Pour supprimer les fichiers infectés. Cette action n'est pas recommandée!
Déplacer en quarantaine	Les fichiers infectés sont déplacés en quarantaine. Lorsque le virus est en quarantaine il ne peut avoir aucune action néfaste.
Renommer	Pour changer l'extension des fichiers infectés. La nouvelle extension des fichiers infectés sera `.vir`. En renommant les fichiers infectés, la possibilité d'exécuter et donc de propager l'infection disparaît. En même temps, ils peuvent être sauvegardés pour un examen et analyse ultérieur.
Demander	Chaque fois qu'un fichier infecté est détecté, une boîte de dialogue est affichée, dans laquelle l'utilisateur peut sélectionner l'action à entreprendre sur ce fichier. Il est recommandé de choisir l'action suivant l'importance du fichier.
Ignorer	Dans ce cas, l'infection est ignorée et aucune action n'est réalisée sur le fichier infecté. Seul son statut sera rapporté.

Sélectionnez la seconde action à prendre sur les fichiers infectés:

Action	Description
Effacer	Supprimer les fichiers infectés automatiquement, sans aucune alerte.
Déplacer en quarantaine	Les fichiers infectés sont déplacés en quarantaine. Lorsque le virus est en quarantaine il ne peut avoir aucune action néfaste.
Renommer	Pour changer l'extension des fichiers infectés. La nouvelle extension des fichiers infectés sera `.vir`. En renommant les fichiers infectés, la possibilité d'exécuter et donc de propager l'infection disparaît. En même temps, ils peuvent être sauvegardés pour un examen et analyse ultérieur.
Demander	Chaque fois qu'un fichier infecté est détecté, une boîte de dialogue est affichée, dans laquelle l'utilisateur peut sélectionner l'action à entreprendre sur ce fichier. Il est recommandé de choisir l'action suivant l'importance du fichier.
Ignorer	Dans ce cas, l'infection est ignorée et aucune action n'est réalisée sur le fichier infecté. Seul son statut sera rapporté.

Cliquez sur **Suivant**.

8. Création du rapport

Choisissez comment créer un fichier de rapport d'analyse.

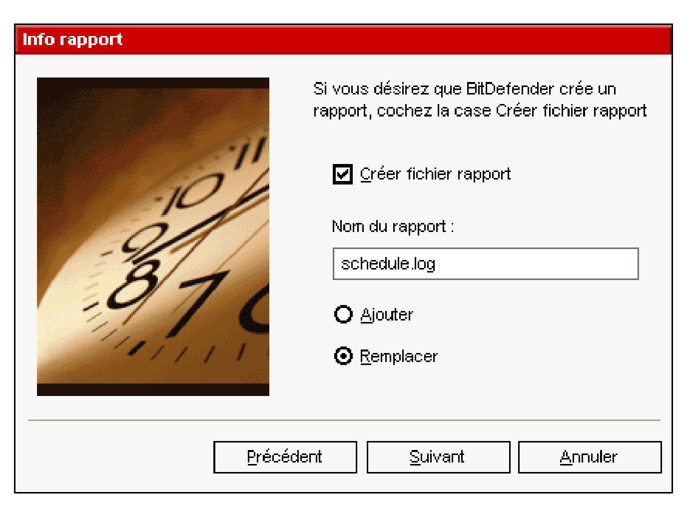


Figure 23

Pour créer un rapport d'analyse, cliquez sur **Créer fichier rapport**. Dès lors, les autres options pour la création d'un fichier rapport seront activées.

Tapez le nom du fichier rapport dans la case **Nom du rapport**. Par défaut, le nom est `schedule.log`. Il contiendra toutes les informations concernant le processus d'analyse : le nombre de virus identifiés, le nombre de fichiers analysés, le nombre de fichiers désinfectés et supprimés.

Cliquez sur **Ajouter** si vous souhaitez ajouter à un fichier rapport existant les informations d'une nouvelle analyse, construisant ainsi un mini historique des résultats des analyses réalisées à différents moments.

Cliquez sur **Remplacer** si vous souhaitez créer un nouveau fichier rapport à chaque nouvelle analyse lancée. Dans ce cas, les informations concernant la précédente analyse seront effacées.

Astuce: Vous pouvez voir le fichier rapport dans la section Rapport du module **Antivirus**.

Cliquez sur **Suivant**.

9. Consulter les propriétés de la tâche

Il s'agit de la dernière étape dans la création d'une tâche d'analyse.

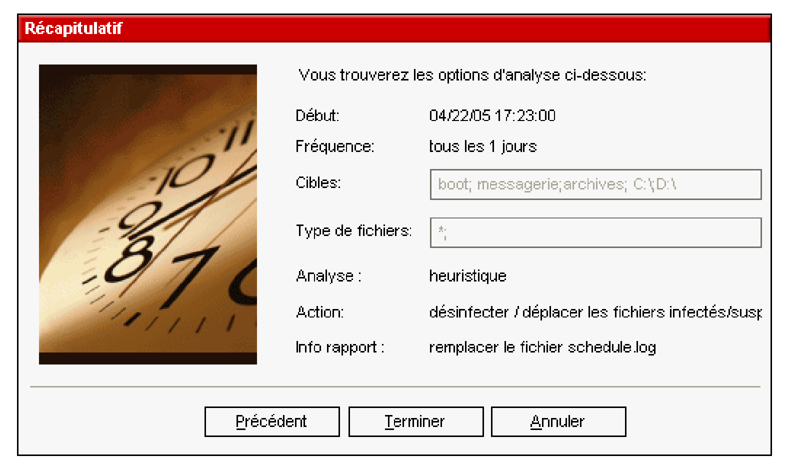


Figure 24

Dans cette fenêtre vous pouvez, voir tous les paramétrages de la tâche d'analyse et vous pouvez les modifier en retournant sur les étapes précédentes (**Précédent**). Si vous ne souhaitez faire aucune modifications, cliquez sur **Terminer**.

La nouvelle tâche apparaîtra dans la section **Planificateur**.

Pour chaque tâche d'analyse programmée, vous pouvez voir son nom, sa description, sa date de démarrage, la prochaine fois qu'elle sera lancée, le type de tâche (périodique ou ponctuelle), la cible, les extensions de fichiers, le type d'analyse et l'action à entreprendre sur les fichiers infectés.

Note

Lors de la modification d'une tâche d'analyse, les mêmes étapes seront suivies. Dans le cas d'une modification du nom de l'évènement, une nouvelle tâche sera créée. Par exemple, si nous avons l'évènement EV1 et que nous avons modifié son nom en EV2, EV1 ne disparaîtra pas, à l'inverse une nouvelle tâche nommée EV2 avec les mêmes propriétés que EV1 apparaîtra.

Si vous faites un clic-droit sur une tâche programmée, un menu s'affichera comme celui ci-dessous:



Figure 25

Si aucun évènement n'est sélectionné, et que vous faites un clic-droit sur la section **Planificateur**, seule l'option Creér sera active, toutes les autres seront inaccessibles.

Astuce: Le **Planificateur** permet un nombre illimité de tâches d'analyse.

Vous pouvez également naviguer à travers les tâches d'analyse en utilisant le clavier : appuyer sur la touche **Delete** pour effacer une tâche, pressez la touche **Enter** afin de voir les propriétés de l'événement sélectionné ou appuyez sur la touche **Insert** pour créer une nouvelle tâche (l'assistant du **Planificateur** se lancera).



Utilisez les touches de navigation pour faire défiler la page de bas en haut et de gauche à droite.

Isoler les fichiers infectés

BitDefender permet d'isoler les fichiers infectés ou suspects dans une zone sécurisée, nommée quarantaine. En isolant ces fichiers dans la quarantaine, le risque d'être infecté disparaît et, en même temps, vous avez la possibilité d'envoyer ces fichiers pour une analyse par le VirusLab de BitDefender. La section qui permet d'administrer ces fichiers isolés est la **Quarantaine**. Ce module a été conçu avec une fonction d'envoi automatique des fichiers infectés au VirusLab.

Dans le cas où vous n'auriez pas encore ouvert la console de management, vous pouvez y accéder depuis le menu Démarrer de Windows en suivant le chemin suivant **Démarrer → Programmes → BitDefender → BitDefender 8 SpamDeny** ou plus rapidement en double-cliquant sur l'icône BitDefender dans la zone de notification.

Dans la console de management, cliquez sur le module **Antivirus** puis sur l'onglet **Quarantaine**.

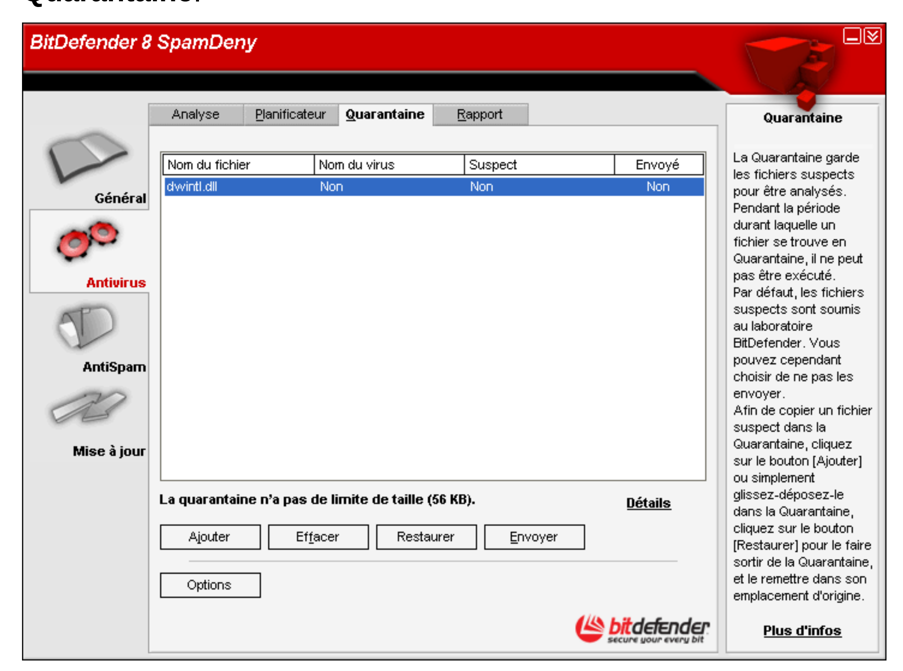


Figure 26

Comme vous le constaterez, la section **Quarantaine** contient une liste de tous les fichiers qui ont été isolés jusque là. Chaque fichier intègre son nom, sa taille, sa date d'isolation et sa date de soumission. Si vous voulez voir plus d'informations à propos des fichiers en quarantaine, cliquez sur **Plus d'infos**.



Note

Lorsque le virus est en quarantaine, il ne peut faire aucun dégât puisqu'il ne peut être exécuté ou lu.

La section **Quarantaine** contient des boutons pour administrer ces fichiers:

- **Ajouter** – ajoute des fichiers à la quarantaine. Utilisez ce bouton pour mettre en quarantaine un fichier que vous soupçonner d'être infecté. Une fenêtre s'ouvrira et vous pourrez sélectionner le fichier depuis son emplacement sur le disque. De cette façon, le fichier est copié en quarantaine. Si vous voulez déplacer le fichier en zone de quarantaine, vous devez cocher la case **Supprimer de l'emplacement d'origine**. Une méthode plus rapide d'ajouter des fichiers suspects à la quarantaine est de les glisser – déposer dans la liste de quarantaine.
- **Supprimer** – supprime les fichiers sélectionnés de votre ordinateur.

- **Restaurer** – remet le fichier sélectionner à son emplacement d'origine.
- **Envoyer** – envoie les fichiers sélectionnés pour analyse au VirusLab. Vous devez spécifier quelques informations pour pouvoir les soumettre. Pour cela, cliquez sur **Paramétrages** et complétez les champs de la section **Paramétrages Emails**, comme décrit ci-dessous.

Note

Par défaut, les fichiers suspects sont soumis pour analyse au VirusLab. Cependant vous pouvez choisir de ne pas les soumettre en désélectionnant l'option **Envoyer automatiquement la quarantaine** depuis les paramétrages de la quarantaine.

- **Options** – ouvre les options avancées pour la zone de quarantaine. La fenêtre suivante s'ouvrira:

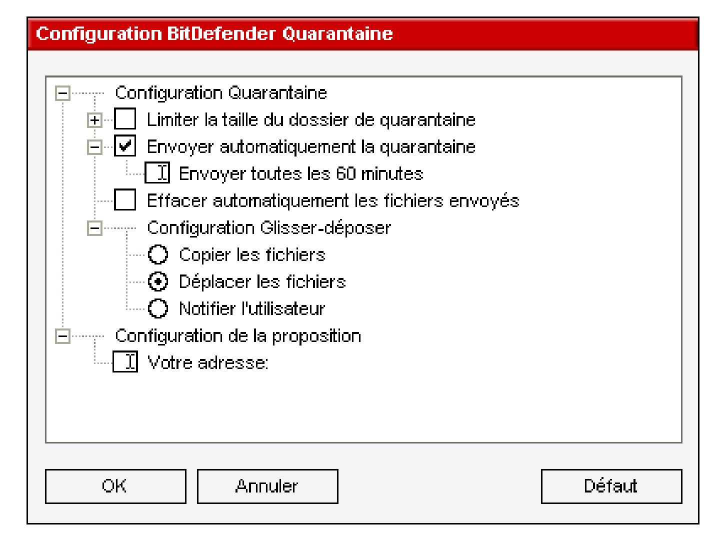


Figure 27

Les options de quarantaine sont groupées en deux catégories:

- **Configuration quarantaine**
- **Configuration de la proposition**

Cliquez sur la case avec un "+" pour ouvrir une option ou la boîte avec un "-" pour fermer une option.

Configuration Quarantaine

- **Limiter la taille du dossier de quarantaine** - maintient sous contrôle la taille de la quarantaine. Cette option est activée par défaut et sa taille est de 12 000 kbs. Si vous voulez changer cette valeur, vous pouvez en introduire une autre dans le champ **La taille maximale du dossier de quarantaine est**.

  L'option **Effacer automatiquement les vieux fichiers** est utilisée pour supprimer les anciens fichiers lorsque la quarantaine est pleine et qu'il n'y a plus de place pour ajouter de nouveaux fichiers.
- **Envoyer automatiquement la quarantaine** – envoie automatiquement les fichiers en quarantaine au VirusLab pour analyse. Vous pouvez paramétrer le délai entre deux envois consécutifs dans le champs **Envoyer toutes les**.
- **Effacer automatiquement les fichiers envoyés** – supprime automatiquement les fichiers en quarantaine après les avoir envoyés au VirusLab pour analyse.
- **Configuration Glisser – déposer** – si vous utilisez la méthode du glisser - déposer pour ajouter de nouveaux fichiers à la quarantaine, vous pouvez ici spécifier l'action : copier, déplacer ou demander à l'utilisateur.

Configuration de la proposition

Vous devez spécifier votre adresse e-mail afin d'envoyer des fichiers en quarantaine au VirusLab.

- **Votre adresse** – entrez votre adresse e-mail dans le cas où vous souhaitez recevoir une réponse de nos experts au sujet des fichiers suspects soumis pour analyse.

Afficher les fichiers rapports

Lors du lancement d'un processus d'analyse, l'utilisateur a la possibilité d'opter pour la création d'un fichier rapport où il peut voir des informations au sujet de l'analyse. L'utilisateur peut voir ces rapports depuis la console de management.

Dans le cas où vous n'auriez pas encore ouvert la console de management, vous pouvez y accéder depuis le menu Démarrer de Windows en suivant le chemin suivant **Démarrer → Programmes → BitDefender → BitDefender 8 SpamDeny** ou plus rapidement en double-cliquant sur l'icône BitDefender dans la zone de notification.

Dans la console de management, entrez dans le module **Antivirus** et cliquez sur l'onglet **Rapports**.

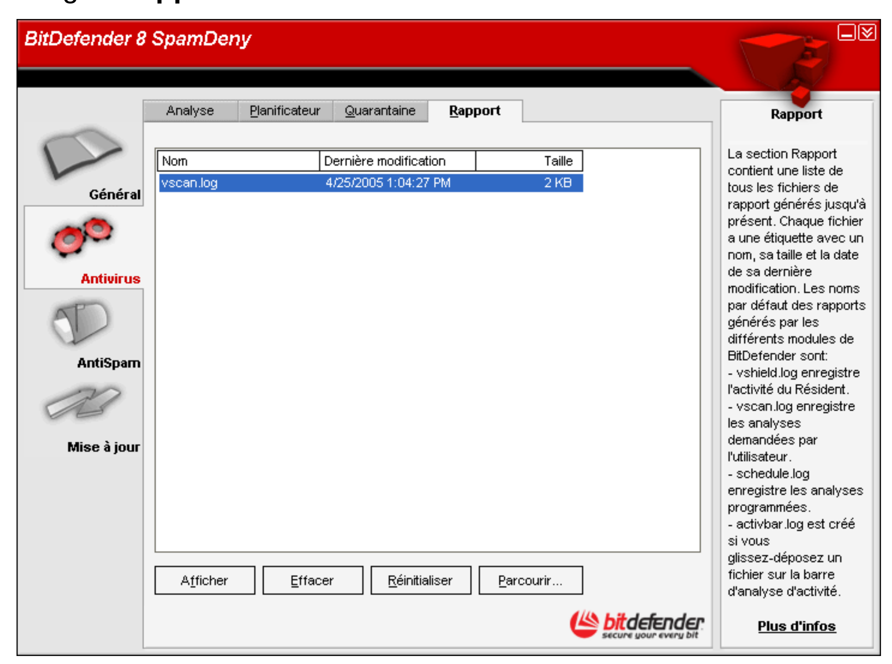


Figure 28

BitDefender conservera des traces de sa propre activité sur votre ordinateur. Les fichiers rapports par défaut sont les suivants:

- Vscan.log est créé lorsque vous scannez immédiatement votre système;
- Schedule.log vient des tâches d'analyse que vous pouvez avoir paramétré;

La section **Rapport** contient une liste de tous les fichiers rapports générés. Chaque fichier a son nom, sa taille et sa date de dernière modification. Il y a des boutons créés pour l'administration de ces fichiers rapports.

La fonction de chacun de ces boutons est expliquée ci-après:

- ➔ **Afficher** – ouvre le fichier rapport sélectionné.
- ➔ **Effacer** – supprime le fichier rapport sélectionné.
- ➔ **Réinitialiser** – si la console de management est ouverte à la section **Rapport** et que vous réalisez dans le même temps une analyse de votre ordinateur, le nouveau fichier rapport avec les résultats d'analyse (si vous avez sélectionné l'option **Créer un fichier rapport**) ne sera visible seulement qu'après avoir cliqué sur **Réinitialiser**.
- ➔ **Parcourir** – ouvre une fenêtre dans laquelle vous pouvez sélectionner le fichier rapport que vous souhaitez voir.

Astuce: Les fichiers rapports sont sauvegardés par défaut dans le répertoire d'installation de **BitDefender**. Si vous avez sauvegardé les fichiers rapports dans un autre répertoire, vous devez utiliser le bouton **Parcourir** pour les localiser.

Désinfection d'un virus détecté

Les virus sont beaucoup plus faciles à arrêter qu'à les désinfecter une fois entrés dans votre PC. C'est pourquoi la protection antivirus devrait être toujours active et mise à jour.

BitDefender détecte un virus résident il est recommandé d'essayer de le désinfecter. Ceci peut être impossible pour une variété de raisons, les virus résidents actifs pouvant être difficiles à gèrer.

Si **BitDefender** trouve un virus et ne peut pas le désinfecter il est recommandé de contacter notre équipe support à l'adresse sav@editions-profil.fr.

Le secret pour la désinfection d'un virus est le connaitre. Vous pouvez trouver des infos sur le virus sur notre site, www.bitdefender.fr.

Pour les virus les plus répandus nous vous offrons des utilitaires spéciaux de désinfection.

C'est toujours une bonne idée de chercher sur internet toute information sur le virus en question.

Contactez notre support technique à l'adresse sav@editions-profil.fr.

Module Antispam

Le spam (courrier non sollicité) est un problème croissant, tant à titre personnel que professionnel. Contenu inadapté aux enfants, contenu illégal, perte de temps…et vous ne pouvez pas stopper ces envois non sollicités, les désinscriptions proposés dans ces emails ne servant la plupart du temps qu'à vérifier la validité de votre adresse et donc à augmenter encore le nombre de spam reçu.

Plus de fonctions

Fonctionnement de BitDefender Antispam

Le schéma du fonctionnement de BitDefender:

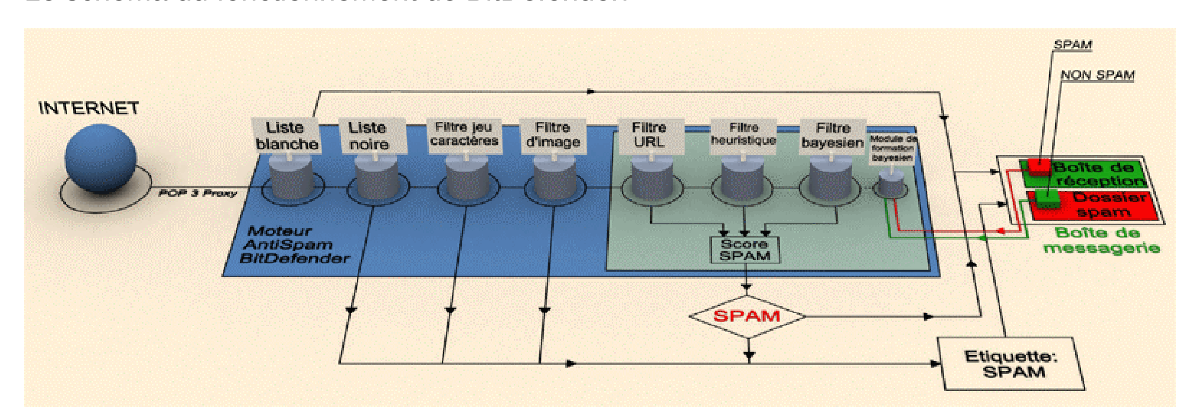


Figure 29

Le moteur BitDefender AntiSpam intègre sept filtres differents qui vous assurent une boîte de réception sans spam: Liste Blanche, Liste Noire, Filtre jeu de caractères, Filtre d'Image, Filtre URL, Filtre Heuristique et Filtre Bayesien.



Vous pouvez activer/désactiver chacun de ces filtres dans le module **Antispam**, section Configuration à partir de la **Console d'Administration BitDefender**.

Tout message provenant de l'Internet est d'abord confronté aux filtres Listes blanche / noire. Si l'expéditeur se trouve dans la liste blanche (des amis) le message est dirigé vers la boîte de réception.

Sinon, le filtre Liste Noire reprendra le message pour vérifier si l'expéditeur se trouve sur cette liste. Le courriel sera marqué comme SPAM et déplacé vers le dossier **SPAM** (localisé dans Outlook) si l'adresse est dans la liste.

Sinon, le filtre Jeu de caractères va vérifier si le texte du message est écrit avec des caractères cyrilliques ou asiatiques. Si tel est le cas, le message sera marqué comme Spam et déplacé vers le dossier SPAM. Si le message ne contient pas ces caractères, il sera passé au filtre des images.

Le Filtre d'Image détecte tous les messages e-mail avec des images ayant contenu de spam.

Le filtre URL cherchera des liens et va comparer les liens trouvés avec ceux de la base de données BitDefender. S'il retrouvera un correspondant il ajoutera un score de SPAM à cet message.

Le filtre heuristique reprendra le mail et effectuera des tests sur toutes les parties composantes du message, cherchant des mots, phrases, liens ou autres caractéristiques du SPAM. Il va ajouter aussi un score de spam au courriel.

Si le message est étiqueté comme SEXUALLY-EXPLICIT dans l'objet, BitDefender le considèrera SPAM.

Le filtre Bayesian va ensuite analyser le message, conformément aux informations statistiques concernant le taux auquel des mots spécifiques apparaissent dans les messages classifiés comme spam par rapport à ceux classifiés comme non-spam (par vous ou par le filtre heuristique). Un score de spam sera ajouté au message.

Si le score de spam combiné (Url + heuristique + bayesien) dépasse le score de SPAM pour un message (défini par l'utilisateur dans la section **Antispam** comme niveau de tolérance), alors le message est considéré **SPAM**.



Note

Si vous utilisez un autre client de messagerie que **Microsoft Outlook** ou **Microsoft Outlook Express** vous devrez créer une règle pour déplacer les messages étiquetés comme SPAM dans un dossier de quarantaine (BitDefender ajoute le préfixe [SPAM] à l'objet du message spam).

Listes blanche / noire

La majorité des utilisateurs communiquent régulièrement avec un groupe de personnes ou reçoivent des messages de la part des entreprises et compagnies du même domaine. Utilisant les listes amis/spammeurs vous pouvez classifier clairement de quelles personnes vous voulez recevoir des messages et quelles personnes éviter).



Les **Listes blanche/noire** sont aussi connues comme **Listes des amis/spammeurs**.

Vous pouvez gérer les listes d'amis/spammeurs depuis la Console d'administration BitDefender ou depuis la barre d'outils BitDefender (dans **Microsoft Outlook** / **Outlook Express**).

Astuce: Nous vous suggérons d'ajouter les noms de vos amis et leurs adresses mail à la liste des Amis. BitDefender ne bloque pas les messages provenant de ces personnes ; pour cela, ajouter des amis vous aide à laisser passer les messages légitimes.

Filtre jeu de caractères

La majorité des messages spam sont écrits utilisant des caractères cyrilliques ou asiatiques. Configurez ce filtre si vous désirez refuser tous messages écrits avec ces caractères.

Filtre des images

Car le détour des filtres heuristiques est devenue une provocation, de nos jours les boîtes de mail sont pleines de plus en plus des messages ayant une image à contenu non-solicité. Pour mettre fin à ce problème croissant, BitDefender a introduit le **Filtre d'Image** qui compare les signatures des images du mail à ceux de la base de données BitDefender. Au cas d'une égalité, le mail sera étiqueté comme spam.

A chaque fois que vous effectuez une mise à jour, de nouvelles signatures d'images seront ajoutées au **Filtre d'Image**.

Filtre URL

La majorité des messages spam contiennent des liens vers différents sites web (qui contiennent plus de publicité et la possibilité de faire des achats, d'habitude). BitDefender a une base de données, qui contient des liens vers ce type de sites.

Chaque lien dans un message sera vérifié dans la base de données. S'il sera retrouvé, +45 sera ajouté au score de spam.

Filtre heuristique

Le filtre heuristique effectue des tests sur tous les composants du message (pas seulement l'en-tête mais aussi le corps du message en html ou texte), cherchant des mots spécifiques, phrases, liens ou autres caractéristiques du spam.

Il détecte aussi les messages contenant SEXUALLY-EXPLICIT dans leur objet. Ces messages seront considérés spam.



A partir du 19 mai 2004, le spam contenant un matériel sexuel doit inclure l'avertissement SEXUALLY-EXPLICIT dans l'objet, contre risque d'amendes. BitDefender considère ces messages **SPAM**.

Astuce: Chaque fois que vous faites une mise à jour, de nouvelles règles sont ajoutées au filtre heuristique; cela aide à l'efficacité du moteur **Antispam**. Afin de vous protéger contre les spammeurs, BitDefender peut effectuer des mises à jour automatiques. Maintenez l'option Mise à jour automatique activée.

Le filtre Bayesien

Le module filtre Bayesien classifie les messages suivant des informations statistiques sur les occurrences de certains mots dans les messages classifiés comme spam comparés avec ceux déclarés non-spam (par l'administrateur ou le filtre heuristique).

Ceci signifie que, par exemple, si un certain mot de 4 lettres - (par exemple un qui commence par c) apparaît plus fréquemment dans le spam, il est normal de supposer qu'il y a une forte probabilité que le prochain message le contenant soit aussi un spam. Tous les mots d'un message sont pris en considération. En synthétisant les infos statistiques, la probabilité générale qu'un message soit spam est calculée.

Ce module présente une autre caractéristique intéressante: il peut être entraîné. Il s'adapte rapidement au type de messages reçus par un certain utilisateur, et enregistre des informations concernant ces messages. Pour fonctionner d'une manière efficace, le filtre doit être entraîné en lui présentant des échantillons de spam et de messages corrects. Parfois le filtre doit être corrigé – aidé à changer d'avis quand il a pris la mauvaise décision.

Vous pouvez corriger le module Bayesien utilisant les boutons **Spam** et **Pas Spam** de la barre d'outils BitDefender (localisée dans **Microsoft Outlook** / **Outlook Express**).

Ces filtres présentés plus en haut (Liste Blanche, Liste Noire, Filtre jeu de caractères, Filtre d'Image, Filtre URL, Filtre Heuristique et Filtre Bayesien) sont utilisés ensemble par le module BitDefender Antispam, afin de déterminer si un message doit aller dans votre **Boîte de réception** ou pas.



Vous pouvez activer/désactiver chacun de ces filtres dans le module **Antispam**, section Configuration de la **Console d'administration BitDefender**.

Configuration de BitDefender Antispam à partir de la Console d'Administration

L'accès à cette console se fait par le menu Démarrer de Windows, en suivant le chemin suivant: **Démarrer → Programmes → BitDefender 8 → BitDefender 8 SpamDeny** ou plus rapidement en double-cliquant sur l'icône BitDefender dans la zone de notification (en bas à droite à côté de l'horloge).

Dans la console, cliquez sur **Antispam**.

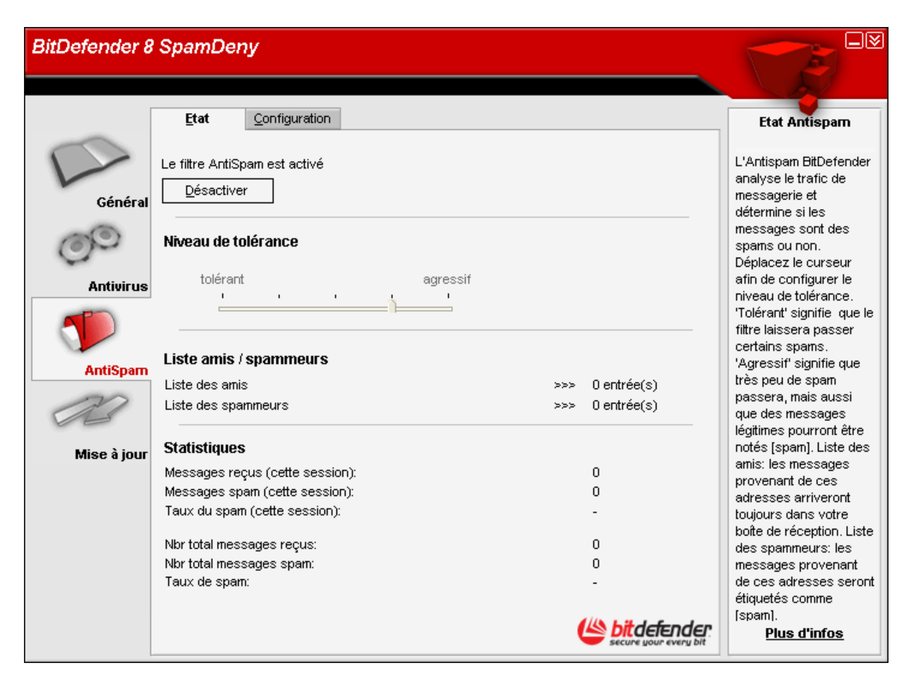


Figure 30

Dans cette section vous pouvez configurer le module Antispam et voir des informations sur son activité. la colonne de droite contient des détails sur les objets soulignés. Afin d'obtenir des informations sur les objets soulignés cliquez-les avec la souris.

Dans la section **Statistiques** vous pouvez consulter les statistiques concernant le module **Antispam**. Ces résultats sont présentés par sessions (depuis que vous avez démarré votre ordinateur) ou vous pouvez consulter un sommaire de l'activité antispam depuis l'installation du filtre **Antispam**.



Pour vous éviter de recevoir du spam, gardez votre filtre **Antispam** activé.

In order to configure the **Antispam** module it is necessary to proceed as follows:

Choisir le niveau d'agressivité

Déplacer le curseur pour modifier la tolérance.

- **Tolérant** - le filtre laissera passer un peu de spam.
- **Agressif** - très peu de spam passera, mais aussi quelques messages légitimes peuvent être considérés spam.

Complétez la liste d'adresses

La liste d'adresses contient des informations sur les adresses e-mail vous envoyant des messages légitimes ou du spam.

➔ **Liste des amis** - Une liste de tous les adresses email de la part de lesquelles vous accepterez les messages, quel que soit leur contenu. Les messages de vos amis ne seront jamais étiquetés comme spam, même si leur contenu ressemble au spam.

Pour gérer la liste d'amis cliquez sur >>> (correspondant à la liste des amis) ou sur le bouton **Amis** de la barre d'outils BitDefender de **Outlook** / **Outlook Express**. La fenêtre suivante contenant les amis apparaît:

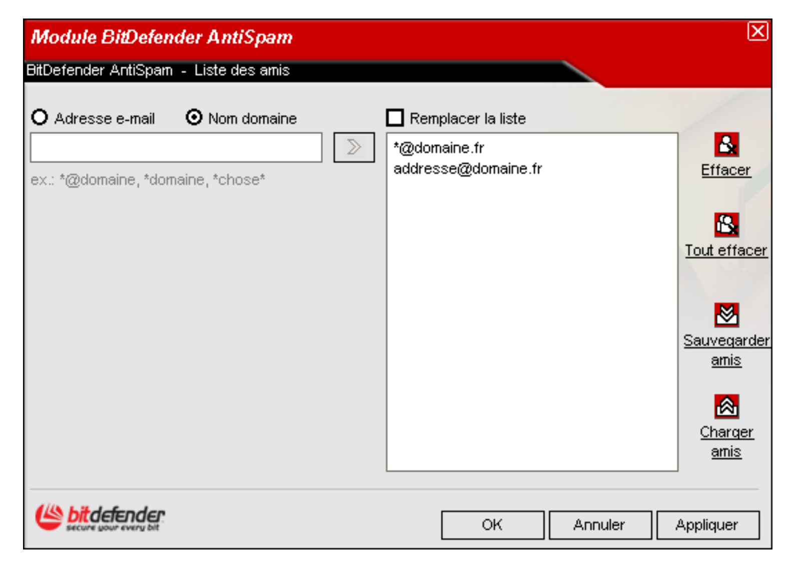


Figure 31

Ici vous pouvez ajouter ou effacer des amis dans la liste.

Si vous désirez ajouter une adresse email cliquez dans le champ **Adresse e-mail**, introduisez-la et cliquez sur .

L'adresse apparaîtra dans la liste d'amis.



L'adresse doit être spécifiée de cette manière: `name@domain.com`.

Si vous désirez rajouter un domaine cliquez sur le champs **Nom domaine**, introduisez-le et puis cliquez sur . Le domaine apparaît dans la liste d'amis.

Le domaine peut être spécifié de ces manières:

- `@domain.com`, `*domain.com` et `domain.com` - tous les messages en provenance de `domain.com` seront dirigés vers votre boîte de réception quel que soit leur contenu;
- `*domain*` - tous les messages provenant de `domain` (quel que soit le suffixe) seront dirigés vers votre boîte de réception quel que soit leur contenu;
- `*com` - tous les messages ayant comme suffixe du domaine seront dirigés vers votre boîte de réception quel que soit leur contenu.



Note

Tout message en provenance d'une adresse de la liste d'amis sera automatiquement dirigé vers votre boîte de réception sans autre investigation.

Pour effacer un objet de la liste, sélectionnez-le et cliquez sur le bouton **Effacer**. Vous pouvez choisir autant d'objets que vous voulez, maintenant appuyée la touche SHIFT ou CTRL. Si vous cliquez sur le bouton **Tout effacer** vous effacerez toutes les entrées de la liste, sans avoir la possibilité de les récupérer.

Utilisez les boutons **Sauvegarder amis** / **Charger amis** pour sauvegarder/charger la liste des amis vers/a partir d'un emplacement désiré. Le fichier a l'extension `.bwl`.

> **Note**
> Nous vous recommandons d'ajouter les noms et adresses e-mail de vos amis dans la **Liste d'amis**. **BitDefender** ne bloquera pas les messages provenant de ces adresses; en conséquence ceci aidera les messages légitimes à vous parvenir.

Cliquez **Appliquer** et **OK** pour sauvegarder et fermer la liste d'amis.

➔ **Liste spammeurs** - Est une liste de toutes les adresses e-mail de la part de lesquelles vous ne voulez recevoir aucun message, quel que soit son contenu.

Pour gérer la liste d'amis cliquez sur >>> (correspondant à la liste des spammeurs) ou sur le bouton **Spammeurs** de la barre d'outils BitDefender de **Outlook** / **Outlook Express**. La fenêtre suivante contenant les amis apparaît:

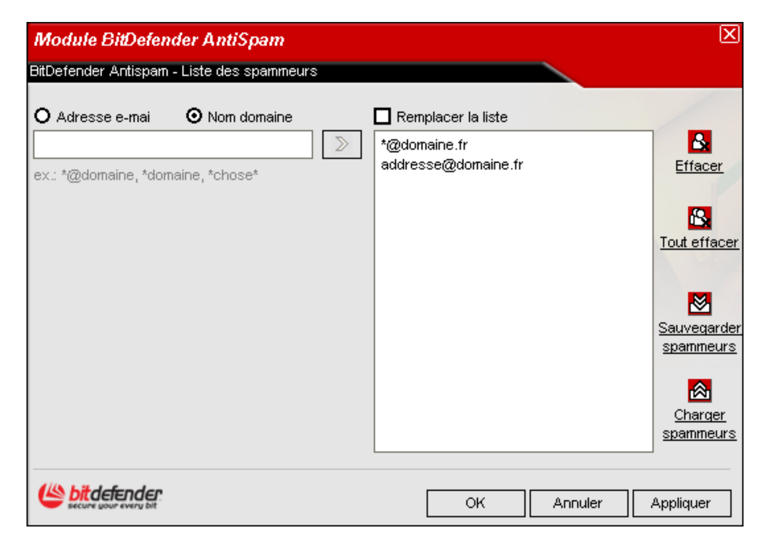


Figure 32

Ici vous pouvez ajouter ou effacer des spammeurs dans la liste.

Si vous désirez ajouter une adresse email cliquez dans le champ **Adresse e-mail**, introduisez-la et cliquez sur ▷.

L'adresse apparaîtra dans la liste des spammeurs.



L'adresse doit être spécifiée de cette manière: `name@domain.com`.

Si vous désirez rajouter un domaine cliquez sur le champs **Nom domaine**, introduisez-le et puis cliquez sur ▷. Le domaine apparaît dans la liste des spammeurs.

Le domaine peut être spécifié de ces manières:

- `@domain.com`, `*domain.com` et `domain.com` - tous les messages provenant de `domain.com` seront étiquetés comme spam;
- `*domain*` - tous les messages de `domain` (quel que soit le suffixe) seront étiquetés comme spam;
- `*com` - tous les messages provenant d'un domaine avec un suffixe `com` seront étiquetés comme spam.



> **Note**
> Tout message en provenance d'une adresse de la liste des spammeurs sera automatiquement marqué [spam] sans autre investigation..

Pour effacer un objet de la liste, sélectionnez-le et cliquez sur le bouton **Effacer** . Vous pouvez choisir autant d'objets que vous voulez, maintenant appuyée la touche SHIFT ou CTRL. Si vous cliquez sur le bouton **Tout effacer** vous effacerez toutes les entrées de la liste, sans avoir la possibilité de les récupérer.

Utilisez les boutons **Sauvegarder spammeurs** / **Charger spammeurs** pour sauvegarder/charger la liste des amis vers/a partir d'un emplacement désiré. Le fichier a l'extension `.bwl`.

Cliquez **Appliquer** et **OK** pour sauvegarder et fermer la liste des spammeurs.

Astuce: Si vous désirez réinstaller BitDefender c'est une bonne idée de sauvegarder la liste **Amis** / **Spammeurs** avant, et la charger après l'installation.

Configuration avancée

Cliquer sur l'onglet **Configuration** afin de consulter et modifier les options avancées pour le module **Antispam**.

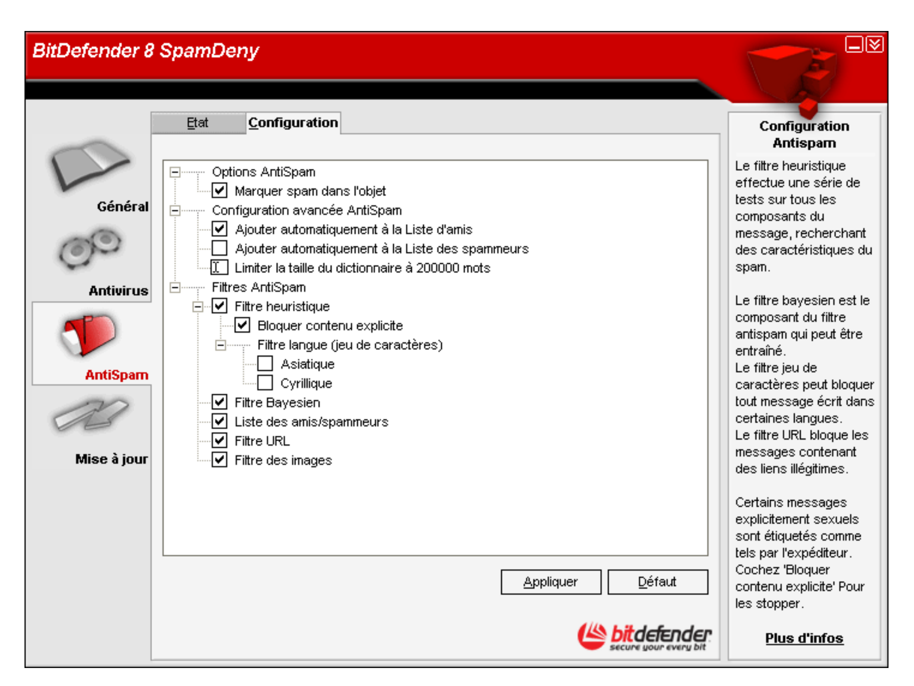


Figure 33

Trois catégories d'options sont disponibles (**Options Antispam**, **Configuration avancée Antispam** et **Filtres Antispam**) organisées dans un menu expansible, similaire aux menus Windows.

Astuce: Cliquez une case "+" pour ouvrir une arborescence et sur une case "-" pour la fermer.

1. Options Antispam

➔ **Marquer spam dans l'objet** – si vous cochez cette option tous les messages étant considérés spam recevront un préfixe [spam] dans leur objet.

2. Configuration avancée Antispam

➔ **Ajouter automatiquement à la Liste d'amis** – si vous la cochez, la prochaine fois que vous cliquerez sur le bouton **Pas Spam** (de la barre d'outils BitDefender de **Microsoft Outlook** / **Outlook Express**) l'expéditeur sera automatiquement ajouté à la liste d'amis.

- **Ajouter automatiquement à la Liste des spammeurs** si vous la cochez, la prochaine fois que vous cliquerez sur le bouton **Spam** (de la barre d'outils BitDefender de **Microsoft Outlook / Outlook Express**) l'expéditeur sera automatiquement ajouté à la liste des spammeurs.



Les boutons **Spam** et **Pas Spam** sont utilisés pour former le filtre Bayesien.

- **Limiter la taille du dictionnaire à 200000 mots** – Avec cette option vous pouvez limiter la taille du dictionnaire bayesien – moindre c'est plus rapide, plus grand c'est plus précis. La taille recommandée est de 200.000 mots.

3. Filtres Antispam

- **Filtre heuristique** – désactive le filtre heuristique.
- **Bloquer contenu explicite** – désactive le filtre contenu explicite.
- **Filtre jeu de caractères (langue)** - ouvre une arborescence dans laquelle vous pouvez choisir de bloquer les messages écrits avec des caractères Cyrillique et/ou Asiatiques.
- **Filtre bayesien** – désactive le filtre bayesien.
- **Liste amis / spammeurs** – désactive les filtres listes d'amis/spammeurs - (liste blanche/noire).
- **Filtre URL** – désactive le filtre URL.
- **Filtre des images** - désactive le filtre des images.

Pour désactiver un filtre, décochez la case à sa gauche ☑ en cliquant dessus. Quand le filtre est inactif la case aura cet aspect ☐.

Cliquez sur **Appliquer** pour enregistrer les modifications. Si vous cliquez sur **Défaut** vous allez charger les paramètres par défaut.

Configuration de BitDefender Antispam à partir de Microsoft Outlook / Outlook Express

Après l'installation, la première fois que vous utilisez **Microsoft Outlook**, un assistant apparaît et vous aide configurer la Liste d'amis et entraîner le Filtre bayesien.

Si vous ne voulez pas le configurer à ce moment, vous pouvez le lancer plus tard à partir de la barre d'outils BitDefender Antispam dans **Microsoft Outlook** / **Microsoft Outlook Express**.

Assistant configuration

Cet assistant vous aide à entraîner le Filtre bayesien, pour améliorer encore l'efficacité de BitDefender Antispam. Vous pouvez aussi ajouter des adresses de votre **Carnet d'adresses** à vos listes d'amis/spammeurs.

1. Fenêtre d'accueil



Figure 34

Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

2. Ajouter des adresses e-mail du Carnet d'adresses à la liste d'amis



Figure 35

Ici vous pouvez voir toutes les adresses de votre **Carnet d'adresses**. Choisissez ceux que vous désirez ajouter à votre Liste d'amis (nous vous recommandons de les rajouter toutes). Vous allez recevoir tous les messages provenant de ces adresses, quel que soit leur contenu.

Choisir **Passer cette étape** si vous voulez passer sans l'appliquer.

Cliquez sur **Suivant**.

3. Effacer les données bayesiennes

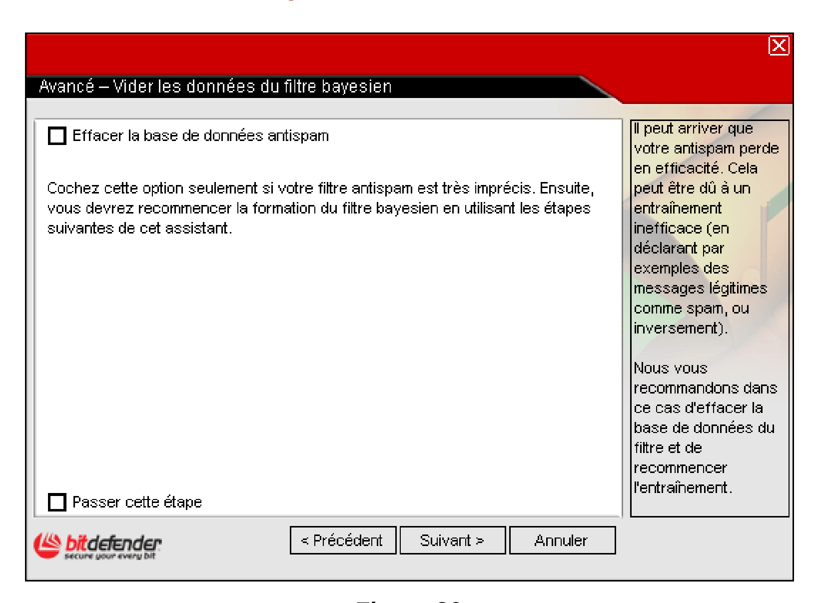


Figure 36

Vous pouvez découvrir que l'efficacité de votre filtre antispam est en baisse. Cela peut être dû à une formation défectueuse. (par ex. vous avez rapporté un nombre de messages légitimes comme spam ou l'inverse). Si votre filtre est très défectueux, vous devriez effacer les données du filtre bayesien et le reformer suivant les étapes ci-dessous:

Choisir **Effacer la base de données antispam** pour initialiser les données du filtre bayesien.

Choisir **Passer cette étape** si vous voulez passer sans l'appliquer.

Cliquer sur **Précédent** pour revenir ou sur **Suivant** pour continuer.

4. Former le filtre bayesien avec des messages légitimes

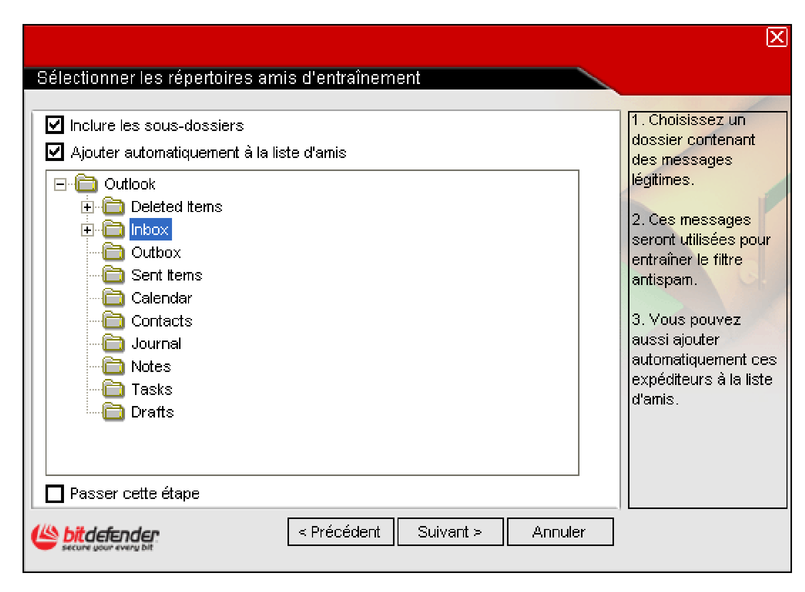


Figure 37

Choisissez un dossier contenant des messages légitimes. Ces messages seront utilisés pour entraîner le Filtre bayesien.

En haut de la fenêtre il y a deux options:

- **Inclure sous-dossiers** – pour inclure les sous-dossiers dans votre choix.
- **Ajouter automatiquement à la liste d'amis** – pour ajouter les expéditeurs à la liste d'amis.

Vous pouvez choisir de **Passer cette étape** cliquant sur cette option.

Cliquez **Suivant**.

5. Former le filtre bayesien avec des messages SPAM

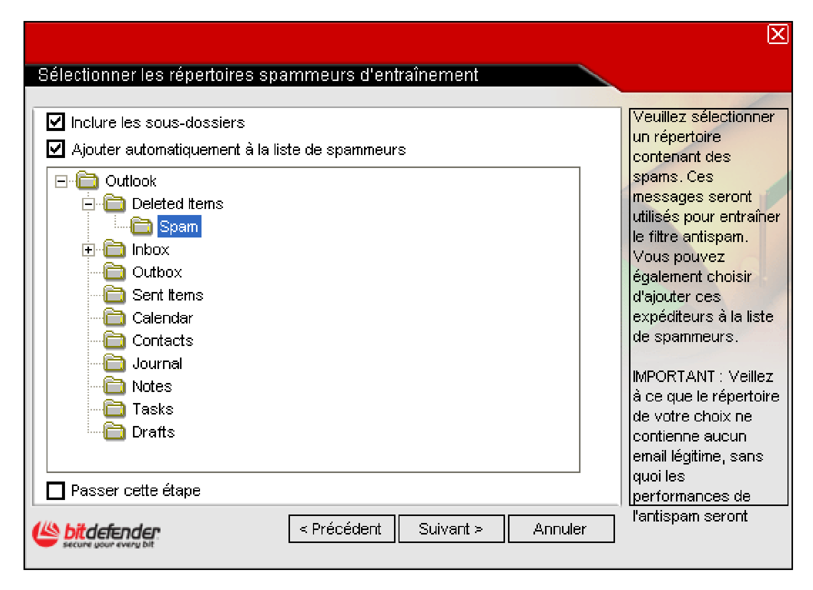


Figure 38

Choisissez un dossier contenant des messages spam. Ces messages seront utilisés pour entraîner le Filtre bayesien.

> ! Vérifiez si le dossier choisi ne contient aucun message légitime, sinon la précision de l'anispam se verra considérablement réduite.

En haut de la fenêtre il y a deux options:

- **Inclure sous-dossiers** – pour inclure les sous-dossiers dans votre choix.
- **Ajouter automatiquement à la liste des spammeurs** – pour ajouter les expéditeurs à la liste de spammeurs.

Vous pouvez choisir de **Passer cette étape** cliquant sur cette option.

Cliquez **Suivant**.

6. Sommaire

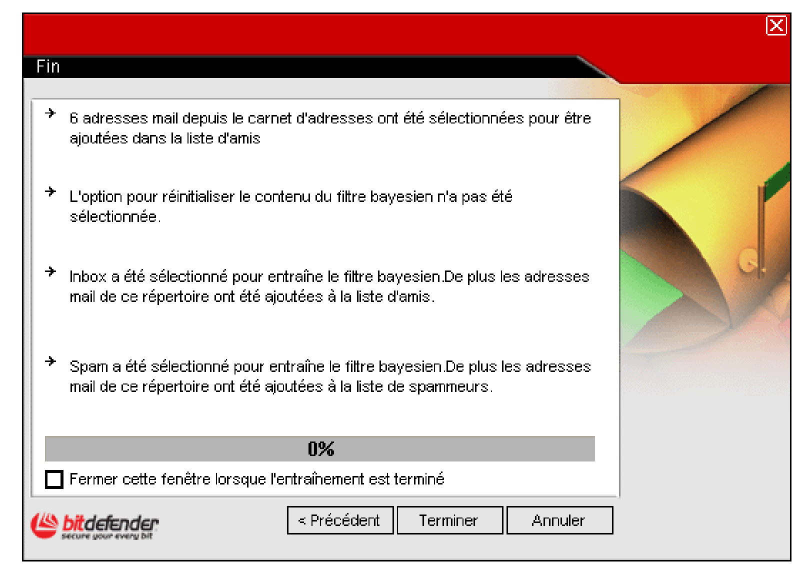


Figure 39

Dans cette fenêtre vous pouvez consulter toute les options faites avec l'assistant de configuration et vous pouvez opérer des choix en retournant aux étapes précédentes (**Précédent**).

Si vous ne voulez faire aucune modification, cliquez sur **Terminer**.

La barre d'outils BitDefender

Vers la haut de **Microsoft Outlook** / **Outlook Express** vous trouverez la barre d'outils de BitDefender créée spécialement pour vous aider configurer BitDefender.



Figure 40

> **Note**
> La principale différence entre BitDefender Antispam pour Microsoft Outlook et Outlook Express est le fait que les messages SPAM sont déplacés dans le dossier Spam de Microsoft Outlook et dans le dossier Effacés pour Outlook Express. Dans les deux cas les messages reçoivent l'étiquette SPAM rajoutée à leurs objets.

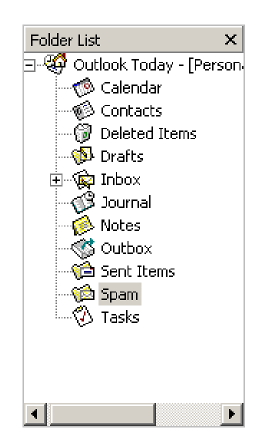


Figure 41

Le dossier **Spam** créé par **BitDefender Antispam** pour **Microsoft Outlook** est situé au même niveau que les objets de la liste répertoires (Calendrier, Contacts, etc).

Chaque bouton sera expliqué ci-dessous:

➔ **Spam** - Cliquez dessus pour envoyer un message au module Bayesien indiquant que le message respectif est spam. Le message recevra l'étiquette SPAM et sera déplacé dans le dossier **Spam**.

Les messages futurs ayant les mêmes caractéristiques seront aussi considérés spam.

Astuce: Vous pouvez choisir un ou plusieurs messages.

➔ **Pas Spam** - Cliquez dessus pour envoyer un message au module Bayesien indiquant que le message respectif n'est pas spam et BitDefender ne devrait pas l'étiqueter. Le message sera déplacé du dossier **Spam** vers la **Boîte de réception**.

Astuce: Vous pouvez choisir un ou plusieurs messages.

Les messages futurs ayant les mêmes caractéristiques ne seront pas considérés spam.



Le bouton **Pas Spam** devient actif quand vous choisissez un message marqué spam par BitDefender (ces messages se trouvent d'habitude dans le répertoire Spam).

➔ **Ajout spammeur** – Cliquez dessus pour ajouter l'expéditeur du message à votre **liste des spammeurs**. La fenêtre suivante apparaît:



Figure 42

Choisir **Ne plus afficher ce message** pour ne plus être demandé lors d'un rajout de spammeur dans la liste.

Cliquez sur **OK** pour fermer la fenêtre.

Les futurs messages provenant de cette adresse seront considérés spam.

Astuce: Vous pouvez choisir un seul expéditeur ou plusieurs.

➔ **Ajout ami** – Cliquez dessus pour ajouter l'expéditeur des messages choisis à votre **Liste d'amis**. La fenêtre suivante apparaît:



Figure 43

Choisir **Ne plus afficher ce message** pour ne plus être demandé lors d'un rajout de ami dans la liste.

Cliquez sur **OK** pour fermer la fenêtre.

Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.

Astuce: Vous pouvez choisir un seul expéditeur ou plusieurs.

➔ **Spammeurs** – Cliquez dessus pour gérer la Liste des spammeurs – elle contient toutes les adresses de la part de lesquelles vous ne voulez pas recevoir des messages, quel que soit leur contenu.

Une fenêtre similaire à celle de la Console d'administration apparaît:

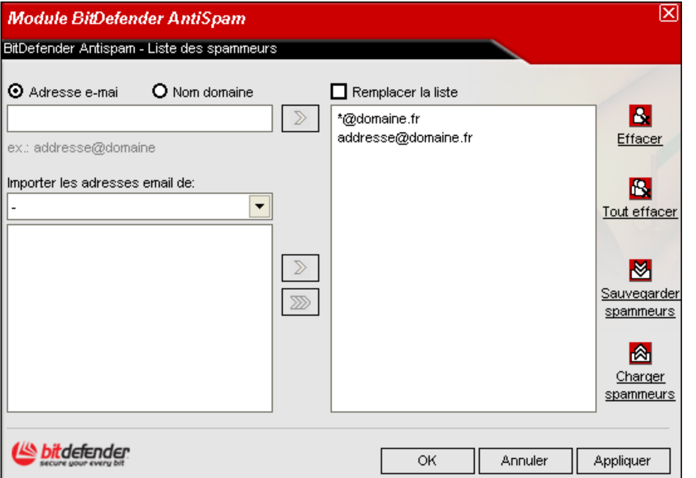


Figure 44

Ici vous pouvez ajouter ou effacer des spammeurs dans la liste.

Si vous désirez ajouter une adresse email cliquez dans le champ **Adresse e-mail**, introduisez-la et cliquez sur .

L'adresse apparaîtra dans la liste de spammeurs.



L'adresse doit être spécifiée de cette manière: `name@domain.com`.

Si vous désirez rajouter un domaine cliquez sur le champs **Nom domaine**, introduisez-le et puis cliquez sur . Le domaine apparaît dans la liste des spammeurs.

Le domaine peut être spécifié de ces manières:

- `@domain.com`, `*domain.com` et `domain.com` - tous les messages provenant de `domain.com` seront étiquetés comme spam;
- `*domain*` - tous les messages de `domain` (quel que soit le suffixe) seront étiquetés comme spam;
- `*com` - tous les messages provenant d'un domaine avec un suffixe `com` seront étiquetés comme spam.

Si vous désirez importer des adresses de messagerie du carnet d'adresses ou de la liste de dossiers, cliquez sur et choisissez **Carnet d'adresses Windows** ou **Répertoire Outlook Express**. Dans la case **Répertoire Outlook Express** une nouvelle fenêtre apparaît:



Figure 45

Choisir le dossier qui contient les adresses e-mail que vous désirez ajouter à la Liste de spammeurs et cliquez sur **Choisir**.

Dans les deux cas les adresses apparaissent dans la liste importée. Choisissez les adresses désirées et cliquez sur [>] pour les rajouter à la Liste de spammeurs. Si vous cliquez sur [>] toutes les adresses seront rajoutées à la liste.

Note

Tout message provenant d'une adresses contenue dans la liste de spammers sera automatiquement marqué Spam.

Pour effacer un objet de la liste, sélectionnez-le et cliquez sur le bouton **Effacer**. Vous pouvez choisir autant d'objets que vous voulez, maintenant appuyée la touche SHIFT ou CTRL. Si vous cliquez sur le bouton **Tout effacer** vous effacerez toutes les entrées de la liste, sans avoir la possibilité de les récupérer.

Utilisez les boutons **Sauvegarder spammeurs** / **Charger spammeurs** pour sauvegarder/charger la liste des amis vers/a partir d'un emplacement désiré. Le fichier a l'extension `.bwl`.

Cochez la case correspondant à **Remplacer la liste** si vous désirez remplacer la **Liste de spammeurs** par celle importee.

Astuce: Si vous désirez réinstaller BitDefender c'est une bonne idée de sauvegarder la liste **Amis** / **Spammeurs** avant, et la charger après l'installation.

Cliquez **Appliquer** et **OK** pour retourner à Outlook.

➔ **Amis** - Cliquez dessus pour gérer la Liste des amis – elle contient toutes les adresses de la part de lesquelles vous voulez recevoir les messages, quel que soit leur contenu.

Une fenêtre similaire à celle de la Console d'administration apparaît:

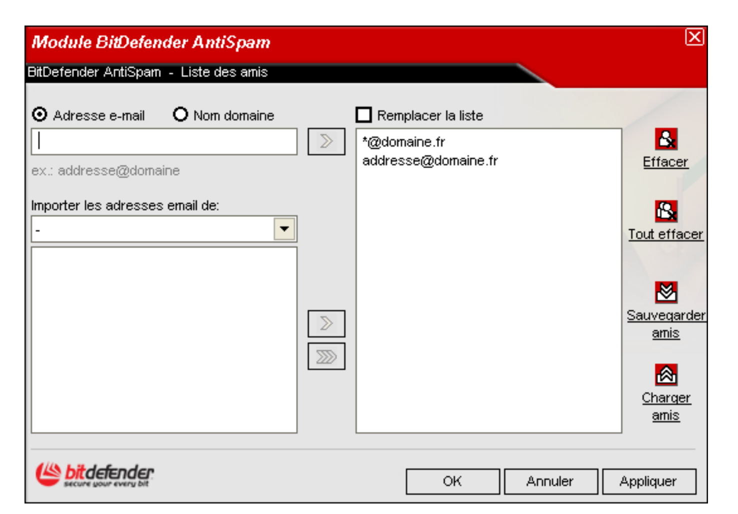


Figure 46

Ici vous pouvez ajouter ou effacer des amis dans la liste.

Si vous désirez ajouter une adresse email cliquez dans le champ **Adresse e-mail**, introduisez-la et cliquez sur [>].

L'adresse apparaîtra dans la liste d'amis.

L'adresse doit être spécifiée de cette manière: `name@domain.com`.

Si vous désirez rajouter un domaine cliquez sur le champs **Nom domaine**, introduisez-le et puis cliquez sur [>]. Le domaine apparaît dans la liste d'amis.

Le domaine peut être spécifié de ces manières:

- `@domain.com`, `*domain.com` et `domain.com` - tous les messages en provenance de `domain.com` seront dirigés vers votre boîte de réception quel que soit leur contenu;
- `*domain*` - tous les messages provenant de `domain` (quel que soit le suffixe) seront dirigés vers votre boîte de réception quel que soit leur contenu;
- `*com` - tous les messages ayant comme suffixe du domaine `com` seront dirigés vers votre boîte de réception quel que soit leur contenu.

Si vous désirez importer des adresses de messagerie du carnet d'adresses ou de la liste de dossiers, cliquez sur ▾ et choisissez **Carnet d'adresses Windows** ou **Répertoire Outlook Express**. Dans la case **Répertoire Outlook Express** une nouvelle fenêtre apparaît:

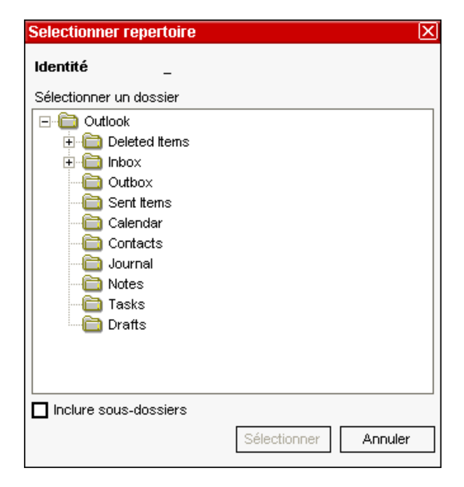


Figure 47

Choisir le dossier qui contient les adresses e-mail que vous désirez ajouter à la Liste d'amis et cliquez sur **Choisir**.

Dans les deux cas les adresses apparaissent dans la liste importée. Choisissez les adresses désirées et cliquez sur [>] pour les rajouter à la Liste d'amis. Si vous cliquez sur [>] toutes les adresses seront rajoutées à la liste.



Note

Tout message en provenance d'une adresse de la liste d'amis sera automatiquement dirigé vers votre boîte de réception sans autre investigation.

Pour effacer un objet de la liste, sélectionnez-le et cliquez sur le bouton **Effacer**. Vous pouvez choisir autant d'objets que vous voulez, maintenant appuyée la touche SHIFT ou CTRL. Si vous cliquez sur le bouton **Tout effacer** vous effacerez toutes les entrées de la liste, sans avoir la possibilité de les récupérer.

Utilisez les boutons **Sauvegarder amis** / **Charger amis** pour sauvegarder/charger la liste des amis vers/a partir d'un emplacement désiré. Le fichier a l'extension `.bwl`.

Cochez la case correspondant à **Remplacer la liste** si vous désirez remplacer la **Liste d'amis** par celle que vous chargez.

Astuce: Si vous désirez réinstaller BitDefender c'est une bonne idée de sauvegarder la liste **Amis** / **Spammeurs** avant, et la charger après l'installation.

Cliquez **Appliquer** et **OK** pour retourner à Outlook.

➔ **Configuration** – cliquez ce bouton pour ouvrir le panneau de configuration.

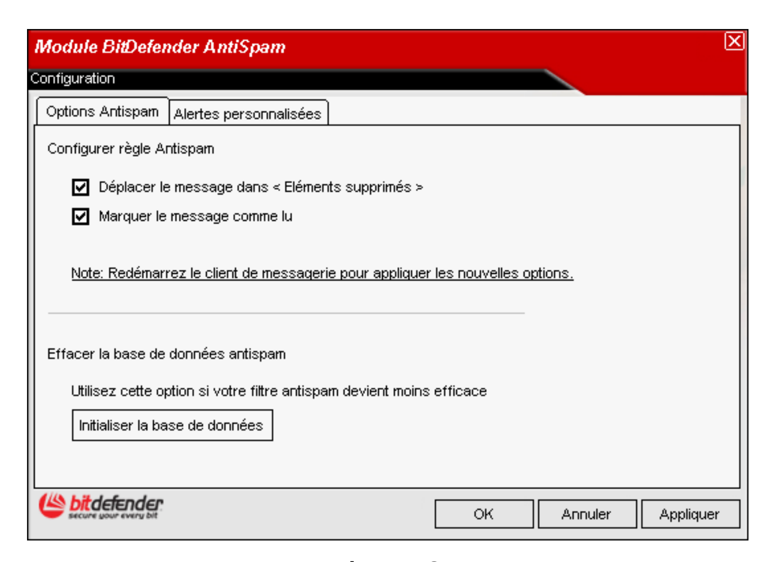


Figure 48

Les options suivantes sont disponibles:

- **Déplacer le message dans <Eléments supprimés>** – pour déplacer les messages spam dans la Poubelle (seulement pour Outlook Express);
- **Marquer le message comme lu** – pour marquer tous les messages spam comme "lus" pour ne pas déranger quand de nouveaux spams arrivent.

Si votre **Filtre Antispam** est très fautif vous devez effacer la base de données du Filtre Bayesien et recommencer à l'entraîner. Cliquez sur **Effacer base antispam** pour le faire.

Cliquez sur l'onglet **Alertes** pour accéder à la section où vous pouvez désactiver l'apparition des fenêtres de confirmation pour Ajout spammer et Ajout ami.

➔ **Assistant** – cliquez dessus pour lancer l'assistant qui vous aidera à former le Filtre bayesien, pour accroître l'efficacité de BitDefender Antispam. Vous pouvez aussi ajouter des adresses de votre carnet d'adresses dans vos Listes d'amis / spammeurs.

➔ **BitDefender Antispam** - cliquez dessus pour ouvrir la Console d'administration.



Si vous voulez cacher la barre d'outils BitDefender, cliquez le droit sur la barre d'outils **Microsoft Outlook** et décochez l'option **BitDefender Antispam Edition**.

Module Mise à jour

De nouveaux virus sont trouvés et identifiés chaque jour. C'est pourquoi il est très important de garder BitDefender à jour avec les dernières signatures de virus. Par défaut, BitDefender recherche automatiquement des mises à jour toutes les trois heures.

Plus de fonctions

Les mises à jour se déclinent en trois parties:

- **Mise à jour pour le moteur antispam** – de nouvelles règles sont ajoutés aux filtres heuristiques et URL; cela permettra d'augmenter l'efficacité de votre Antispam. Ces mises à jour sont affichées sous le nom **Antispam Update**;

- **Mise à jour produit** – lorsqu'une nouvelle version du produit est prête, de nouvelles fonctions et techniques d'analyse sont introduites afin d'augmenter les performances du produit. Ces mises à jour sont affichées sous le nom de **Product Update**;

- **Mise à jour des moteurs antivirus** – comme de nouvelles menaces apparaissent, les fichiers contenant les signatures de virus doivent être mis à jour en permanence contre elles. Elles s'affichent sous le nom de **Virus Definitions Update**.

De plus, du point de vue de l'intervention de l'utilisateur, nous proposons:

- **Mise à jour manuelle** – vérifiant l'existence d'une mise à jour à la demande de l'utilisateur;

- **Mise à jour automatique** – l'antivirus contacte automatiquement le serveur BitDefender afin de vérifier si une mise à jour est disponible. Si c'est le cas, BitDefender est actualisé automatiquement.

Si vous êtes connecté à Internet par câble ou DSL, BitDefender se charge de cela lui-même : Il recherche de nouvelles signatures de virus lorsque vous démarrez votre ordinateur puis ensuite toutes les **3 heures**. Si de nouvelles signatures de virus sont disponibles, BitDefender se met à jour lui-même.

Astuce: Si vous êtes connecté à Internet par une connexion RTC (ou Numéris), alors c'est une bonne idée que de prendre l'habitude de rechercher manuellement des mises à jour.

Mise à jour manuelle

Si vous n'avez pas encore ouvert la console de management, vous pouvez y accéder depuis le menu Démarrer de Windows, en suivant le chemin **Démarrer → Programmes → BitDefender 8 → BitDefender 8 SpamDeny** ou plus rapidement en double-cliquant sur l'icône BitDefender dans la zone de notification.

Dans la console de management, cliquez sur **Mise à jour**.

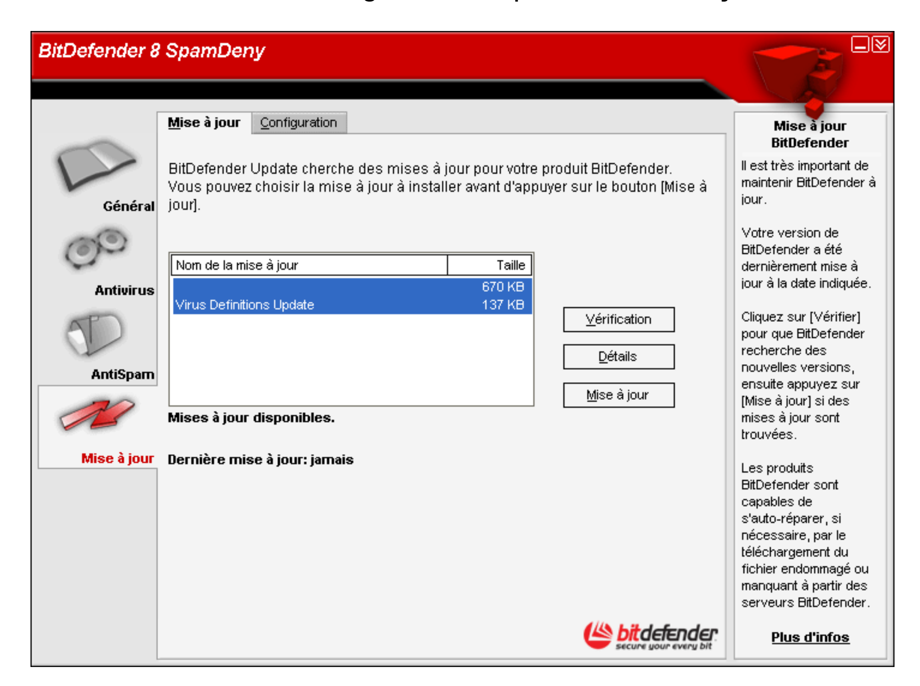


Figure 49

La mise à jour manuelle peut être lancée à tout moment, même si le produit était configuré en mise à jour automatique. Pour mettre à jour manuellement le produit, suivez ces étapes:

- Cliquez sur **Vérification**. Le module **Mise à jour** se connectera au serveur BitDefender et vérifiera la disponibilité d'une mise à jour.
- Si une mise à jour est détectée, son nom et sa taille seront affichés. Cliquez sur **Mise à jour** pour démarrer le processus de mise à jour.

Astuce: Si vous souhaitez voir quels fichiers seront mis à jour, cliquez sur **Détails**.

Si aucune mise à jour n'est détectée le message suivant apparaîtra **Aucune mise à jour disponible!**.



Note

Il peut être nécessaire de redémarrer votre PC lorsque vous avez terminé une mise à jour. Nous vous recommandons de le faire dès que possible.

Mise à jour automatique

Si vous êtes un utilisateur avancé, cliquez sur l'onglet **Configuration** afin de configurer le module **Mise à jour**.

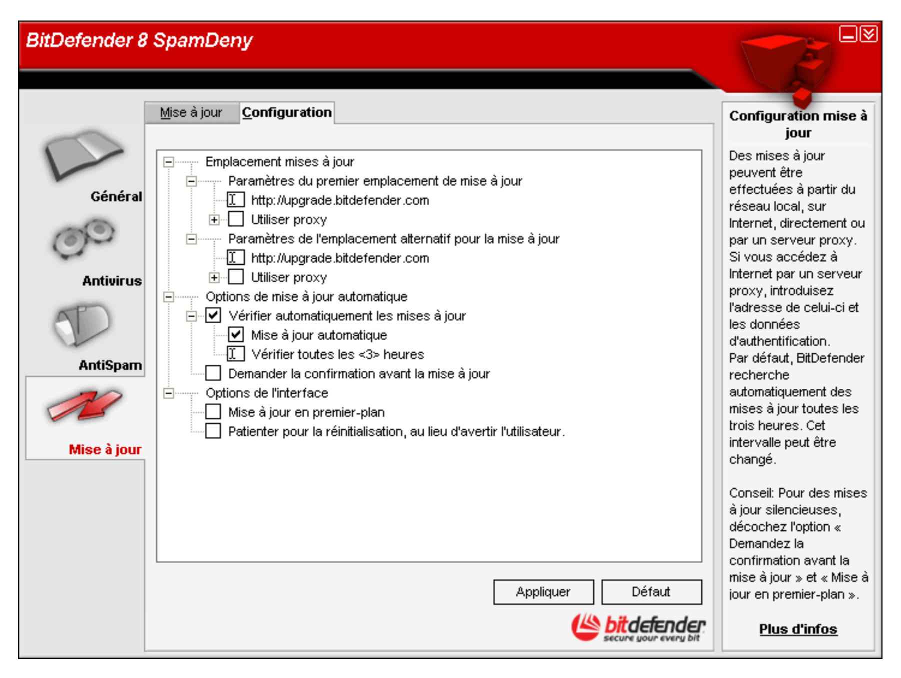


Figure 50

Les mises à jour peuvent être réalisées depuis le réseau local, depuis Internet, directement ou à travers un serveur proxy.

La fenêtre avec les paramétrages de mises à jour contient trois catégories d'options (**Emplacement mises à jour, Options de mise à jour automatique, Options de l'interface**) organisées en menus extensibles, similaires à ceux de Windows.

Cliquez sur la case "+" pour ouvrir une option ou sur celle "-" pour fermer une option.

Emplacement mises à jour

Pour des mises à jour plus rapides et plus fiables, vous pouvez établir deux locations de mise à jour : une **Location Principale de mise à jour** et une **Location Alternative de mise à jour**. Pour les deux, vous devez établir les options suivantes:

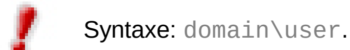
➔ Si vous êtes connectés à un réseau local sur lequel sont placées les signatures de virus de BitDefender, vous pouvez changer l'emplacement des mises à jour ici. Par défaut, c'est le suivant: http://upgrade.bitdefender.com.

➔ **Utilisez proxy** – Dans le cas où la société utilise un serveur proxy, cochez cette option. Les paramétrages suivants doivent être spécifiés.

- **Serveur proxy** – tapez l'IP ou le nom du serveur proxy et le port que BitDefender doit utiliser pour se connecter au serveur proxy.

  ! Syntaxe: `name:port` ou `ip:port`.

- **Utilisateur** – tapez ici un nom d'utilisateur reconnu par le proxy.



Syntaxe: `domain\user`.

- **Mot de passe** – tapez ici un mot de passe valide pour l'utilisateur précédemment spécifié.

Options de mise à jour automatique

➔ **Vérifier automatiquement les mises à jour** – Cela assure que BitDefender contrôle automatiquement nos serveurs pour la disponibilité de mises à jour.

- **Mise à jour automatique** – Si BitDefender détecte une nouvelle mise à jour sur nos serveurs, alors avec cette option cochée, BitDefender télécharge et implémente la mise à jour.

- **Vérifier toutes les <x> heures** – Paramétrez la fréquence de recherche de mise à jour de BitDefender. L'intervalle de temps par défaut est de 3 heures.

➔ Gardez sélectionné **Demander confirmation avant mise à jour** si vous souhaitez être interrogé avant le téléchargement et l'installation des mises à jour.

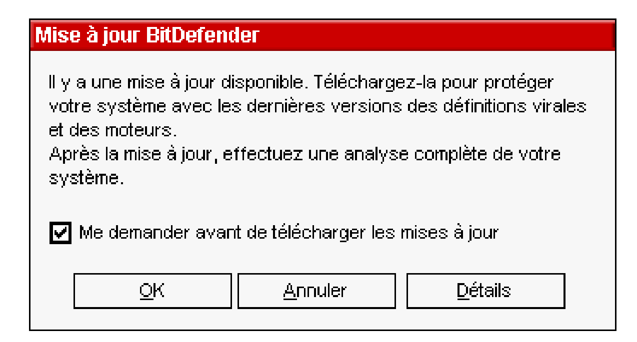


Figure 51

Cliquez sur **OK** pour démarrer le processus de mise à jour, cliquez sur **Détails** pour voir quels fichiers seront actualisés ou cliquez sur **Annuler** pour mettre à jour plus tard.

Options de l'interface

➔ **Mise à jour en premier plan** – Par défaut la mise à jour du produit se fait en arrière plan. Si vous souhaitez que la fenêtre de mise à jour soit par dessus les autres fenêtres, utilisez cette option.

➔ **Patientez pour la réinitialisation, au lieu d'avertir l'utilisateur** - Si une mise à jour nécessite la réinitialisation, le produit utilisera les fichiers anciens jusqu'à la réinitialisation du système. L'utilisateur ne sera pas averti sur la réinitialisation, c'est pourquoi le processus de mise à jour de BitDefender ne perturbera pas le travail de l'utilisateur.

Cliquez sur **Appliquer** pour enregistrer les modifications. Si vous cliquez sur **Défaut** vous allez charger les paramètres par défaut.

5

Meilleurs conseils

Antispam

Etapes à suivre pour éviter de recevoir du spam:

1. Si vous utilisez Microsoft Outlook ou Microsoft Outlook Express, utilisez l'assistant de configuration qui apparaît la première fois que vous accédez à votre client de messagerie. Vous pouvez aussi le lancer à partir de la barre d'outils BitDefender en cliquant sur le bouton **Assistant**.

2. **Ajouter les adresses des gens de la part de lesquels vous voulez recevoir tout message à la liste d'amis** – Nous vous recommandons d'ajouter les noms et adresses e-mail de vous amis à la Liste des amis. BitDefender ne bloquera aucun de leurs messages; l'ajout des amis à la liste assure la transmission des messages légitimes.

3. **Former le filtre bayesien** – Chaque fois que vous recevez un message que vous considérez spam, mais BitDefender ne l'étiquette comme tel, sélectionnez-le et cliquez le bouton **Spam** de la barre d'outils BitDefender. Les messages futurs ayant les mèmes caractéristiques seront étiquetés [SPAM].

   Le filtre bayesien s'active seulement après lui avoir montré au moins 60 messages légitimes. Pour le faire, vous devez recourir à l'assistant de configuration.

4. **Maintenir BitDefender mis à jour** – Chaque fois que vous faites une mise à jour de nouvelles règles seront rajoutées au filtre heuristique et de nouveaux liens seront rajoutés au filtre URL. Cela aide à accroître l'efficacité de votre moteur Antispam.

5. **Configuree le filtre jeu de caractères** – La plupart des messages spam sont écrits avec des caractères cyrilliques ou asiatiques. Configurez ce filtre pour rejeter tout message utilisant ces caractères.

Astuce: Vous pouvez activer/désactiver chaque filtre antispam dans le module **Antispam**, section Configuration de la **Console d'administration BitDefender**.

6

Questions courantes

Général

1. **Q:** Comment faire pour vérifier que BitDefender fonctionne vraiment?
R: Dans le module **Général**, cliquez sur l'onglet Etat et regardez les statistiques.

2. **Q:** Quelles sont les demandes de système?
R: Vous trouverez les demandes de système dans la section Installation.

3. **Q:** Comment désinstaller BitDefender?
R: Suivez: **Démarrage** → **Programmes** → **BitDefender 8** → **Modifier, réparer ou désinstaller** et dans la fenêtre qui apparaît cliquez sur **Désinstaller**. Cela démarre le processus de désinstallation.

4. **Q:** Où introduire la clef d'activation (code d'activation)?
R: Dans le module **General**, cliquez sur l'onglet Enregistrer et cliquez sur **Introduire code d'activation**.

Antivirus

5. **Q:** Comment effectuer une analyse complète du système?
R: Dans le module **Antivirus**, cliquez sur l'onglet Analyse, cochez **Disques locaux** et ensuite **Analyse**.

6. **Q:** Combien de fois par semaine je devrais analyser mon PC?
R: Nous recommandons une fréquence d'au moins une fois par semaine.

7. **Q:** Comment analyser automatiquement tout fichier que je transfère dans mon PC?
R: BitDefender analyse tous les fichiers à l'accès. Vous devez seulement maintenir Résident activé.

8. **Q:** Comment programmer BitDefender à analyser mon PC périodiquement?
R: Dans le module **Antivirus**, cliquez sur Planificateur, sur **Nouveau** et suivez l'assistant.

9. **Q:** Qu'est-ce qui se passe avec les fichiers de la quarantaine?
R: Vous pouvez les envoyer aux Laboratoires BitDefender pour analyse, mais d'abord il vous faut établir la configuration de messagerie (dans la section Quarantaine – cliquez sur **Configuration**).

Antispam

10. **Q:** Qu'est-ce que c'est le spam?
R: Le Spam sont les messages commerciaux non-sollicités.

11. **Q:** Comment fonctionne BitDefender Antispam?
R: Consultez ce schéma de fonctionnement dans le guide utilisateur.

12. **Q:** Où va le spam?
R: Si vous utilisez **Microsoft Outlook** / **Microsoft Outlook Express**, les messages spam sont déplacés dans le répertoire Spam / Effacés.

Astuce: Si vous utilisez un autre client de messagerie vous devriez créer une règle pour déplacer les messages considérés Spam par BitDefender dans un dossier de quarantaine de votre choix. BitDefender ajoute le préfixe [SPAM] au sujet des messages considérés comme tels.

13. **Q:** J'ai bloqué une adresse de messagerie mais je continue à recevoir des messages de cette adresse, pourquoi?
R: Si vous continuez à recevoir des messages de cette adresse, vérifiez qu'elle n'est pas dans la Liste d'amis aussi. La **Liste d'amis** a priorité sur la Liste de spammeurs.

14. **Q:** Qu'est-ce que la Liste d'amis (liste blanche)?
R: C'est une liste de toutes les adresses e-mail de la part de lesquelles vous voulez recevoir des messages, quel que soit leur contenu.

15. **Q:** Qu'est-ce que la Liste de spammeurs (liste noire) ?
R: C'est une liste de toutes les adresses e-mail de la part de lesquelles vous ne voulez recevoir aucun message, quel que soit leur contenu.

16. **Q:** Qu'est-ce que le Filtre jeu de caractères?
R: C'est un filtre qui bloque tous les messages écrits en caractères cyrilliques et/ou asiatiques.

17. **Q:** Qu'est-ce que le Filtre URL?
R: C'est un filtre qui cherche des messages avec des liens et les compare avec ceux trouvés dans une base de données URL BitDefender. S'il trouve le lien, +45 sera rajouté au score de spam.

18. **Q:** Qu'est-ce que le Filtre heuristique?
R: C'est un filtre qui effectue un set de tests sur tous les composants du message (pas seulement l'en-tête mais aussi le corps du message en HTML ou texte), cherchant des mots, des phrases, des liens ou autres caractéristiques du spam. Le résultat est un score spam ajouté au message.

19. **Q:** Qu'est-ce que le Filtre Bayesien?
R: C'est un filtre qui clasifie les messages suivant des statistiques concernant le taux d'aparition de certains mots dans les messages habituellement consid'erés comme spam par rapport a ceux légitimes.

Mise à jour

20. **Q:** Pourquoi est-il nécessaire de mettre à jour BitDefender?
R: Chaque fois que vous faites une mise à jour, de nouvelles signatures virales sont rajoutées aux moteurs d'analyse, et de nouvelles règles aux filtres heuristiques et URL.

21. **Q:** Comment mettre à jour BitDefender?
R: Par défaut, BitDefender se met à jour automatiquement toutes les 3 heure. Vous pouvez changer cette option ou faire la Mise à jour manuellement.

7

Glossaire

ActiveX	ActiveX est un modèle pour écrire des programmes tels que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour faire des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent demander ou répondre à des questions, utiliser des boutons et interagir d'autres façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic. Active X est reconnu pour un manque total de commandes de sécurité; les experts en sécurité informatique déconseillent son utilisation sur Internet.
Applete Java	Il s'agit d'un programme Java conçu pour s'exécuter seulement dans une page Web. Pour utiliser une applette dans une page Web, vous devez spécifier le nom de l'applette et la taille (la longueur et la largeur - en pixels) qu'elle peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applette depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applettes diffèrent des applications dans le fait qu'elles sont dirigées selon un protocole de sécurité strict. Par exemple, bien que les applettes s'exécutent sur le client, elles ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applettes sont également limitées pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.
Archive	(1) Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés. (2) Un fichier qui contient un ou plusieurs fichiers dans un format compressé.
Backdoor	Il s'agit d'une faille dans la sécurité d'un système délibérément laissé en place par des développeurs ou mainteneurs. La motivation n'est pas toujours négative; quelques logiciels permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.
Chemin	1. Les directions exactes vers un fichier. Ces directions sont décrites d'habitude par arborescence, de haut en bas, comportant le disque, dossier, sous-dossier, fichier, extension du fichier: c:\jobscompany\note.txt. Ce kit d'informations est un chemin complet. 2. La connexion entre deux points, telle le canal de communication entre deux ordinateurs.
Client de messagerie	Un client de messagerie est un logiciel qui vous permet d'envoyer et recevoir des messages (e-mails).

Cookie	Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une épée à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent (vous voyez seulement des annonces vous intéressant) mais d'autre part, cela implique en réalité "le pistage" et "le suivi" d'où vous allez et de ce sur quoi vous cliquez sur Internet. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple " numéro SKU " (vous savez, le code barres à l'arrière des produits). Bien que ce point de vue puisse paraître extrême, dans certains cas cette perception est justifiée.
Définition virus	La "signature" binaire du virus, utilisé par l'antivirus pour la détection et l'élimination du virus.
Disk drive	C'est une appareil qui lit et écrit des données sur un disque. Une **unité de disque dur** lit et écrit sur un disque dur. Un **lecteur de disquette** accède à des disquettes. Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).
Evénements	Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme l'analyse de la mémoire. Le Scheduler est un outil qui vous aide à programmer vos tâches d'analyse.
Extension de fichier	La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier. De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS Dos. Elles comportent communément une à trois lettres (certains vieux OS ne supportent pas plus de trois). Exemples: "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.
Fausse alerte	Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.
Fichier journal	Un fichier qui enregistre les actions qui surviennent. Par exemple, BitDefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.
Heuristique	Méthode permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter des variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

IP	**Protocole Internet** - Un protocole routable de la suite de protocoles TCP/IP qui se charge de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.
Ligne de commande	Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.
Mémoire	Zone de stockage interne dans votre ordinateur. Le terme *mémoire* regarde le stockage des données dans les "chips" (composants), et le terme *stockage* regarde les disques. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.
Messagerie électronique	Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.
Mise à jour	Une nouvelle version du logiciel ou d'un produit hardware, destinée à remplacer une ancienne version du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, sinon la mise à jour ne se fait pas. BitDefender comporte un module spécial pour la mise à jour. Ce module vous permet de chercher manuellement les mises à jour ou de faire la mise à jour automatiquement.
Navigateur	Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les deux navigateurs les plus populaires sont Netscape Navigator et Microsoft Internet Explorer. Les deux sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugins) pour certains formats.
Non-heuristique	Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut paraître un virus et ne génère donc pas de fausses alertes.
Objets menu démarrage	Tous les fichiers placés dans ce dossier s'ouvrent au démarrage. Par exemple, un écran de démarrage, un fichier son pour quand l'ordinateur démarre, un calendrier, des programmes, peuvent être placées dans ce dossier. D'habitude c'est un raccourci vers le fichier qui est mis dans le dossier, et pas le fichier.
Port	(1) Une interface de l'ordinateur à laquelle vous pouvez connecter un périphérique. Les PCs comportent plusieurs sortes de ports. A l'intérieur, quelques ports pour la connexion des disques, cartes vidéo, ... A l'extérieur, les PCs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques. (2) Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Programmes empaquetés	Un fichier comprimé. Beaucoup de plates-formes et applications contiennent des commandes vous permettant de comprimer un fichier pour qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide". Normalement, cela nécessite 10 octets. Pourtant, un logiciel qui comprime les fichiers remplace la série d'espaces par un caractère spécial série d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.
Script	Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.
Secteur de boot	Un secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge la plate-forme.
System tray	Introduit avec Windows 95, le system tray se situe dans la barre de tâches Windows (à côté de l'horloge) et contient des icônes miniatures pour des accès faciles aux fonctions système: fax, imprimante, modem, volume etc. Double cliquez ou clic droit sur une icône pour voir les options.
Téléchargement	Copier des données (généralement un fichier entier) d'une source principale à un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.
TCP/IP	Transmission Control Protocol/Internet Protocol - Un ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés avec divers architectures hardware et diverses plates-formes. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.
Trojan	Un programme destructif qui prétend être une application normale. Les Trojans ne sont pas des virus et ne se repliquent pas, mais peuvent être tout aussi destructifs. Un des types les plus répandu de Trojans est un logiciel prétendant désinfecter votre PC (mais au lieu de faire cela il l'infecte). Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Trojans, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.
Ver Internet	Un programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure qu'il se propage. Il ne peut pas s'attacher aux autres programmes.
Virus	Un programme ou morceau de code qui est chargé dans votre ordinateur sans que vous le sachiez et fonctionne contre votre gré. La plupart des virus peuvent se répliquer. Tous les virus sont

	crées par des personnes. Un virus simple peut faire une copie de lui-même très vite et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est capable de se transmettre via un réseau par exemple.
Virus de boot	Un virus qui infecte le secteur de boot d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus de boot rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.
Virus macro	Un type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent des langages macro. Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.
Virus polymorphique	Un virus qui change de forme avec chaque fichier qu'il infecte. Comme ils n'ont pas une forme unique bien définie, ces virus sont plus difficiles à identifier.

8

Informations contact

LE SUPPORT TECHNIQUE:

SOFTWIN et Editions Profil s'efforcent de fournir à ses clients des réponses rapides et précises à vos questions. Le Centre de Support, dont vous pouvez consulter les coordonnées ci-dessous, est actualisé en continu et vous donne accès aux toutes dernières descriptions des virus et aux questions les plus fréquemment posées afin de vous répondre en temps utile.

Support technique:

- Par Email: sav.bitdefender@editions-profil.fr
- Par Chat on-line 24h/24 - 7j/7: www.bitdefender.com
- Par courrier: Editions Profil - 49 rue de la Vanne - 92120 Montrouge

Contacts Commercial et Administratif:

commercial@editions-profil.fr

BitDefender 8 SpamDeny

SOFTWIN
Str. Fabrica de Glucoza, Nr.5
Bucuresti, Sector 2, CP 52-93
ROMANIA
0040-21-233 07 80

www.bitdefender.fr



Le support technique téléphonique n'est pas accessible aux personnes disposant d'une version shareware de BitDefender ou d'une version livrée en standard avec un ordinateur (OEM).